what's inside

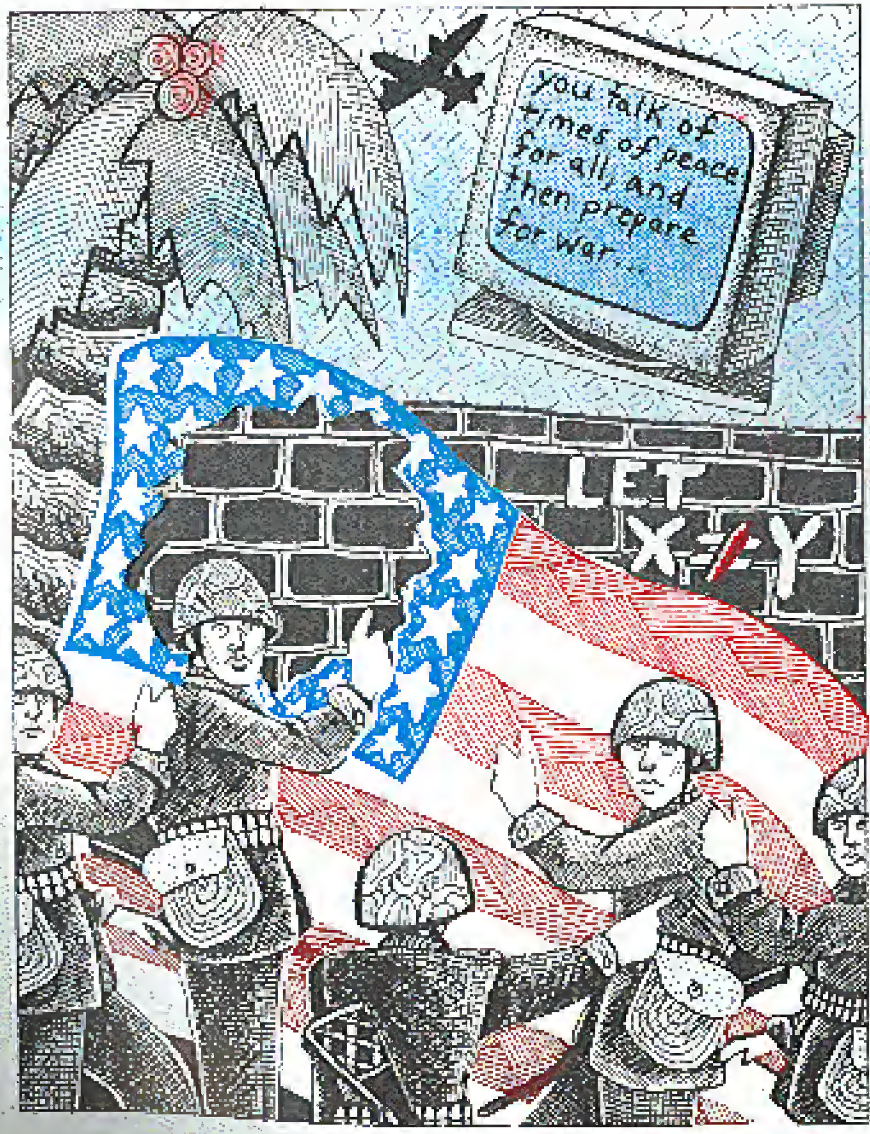
(WE KNOW — This issue should have been out in December, but we wanted to wait for the AT&T story to break. Sorry.)

SECOND CLASS POSTAGE
[illegible]
[illegible]
11733
(ISSN 0749-3851)

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

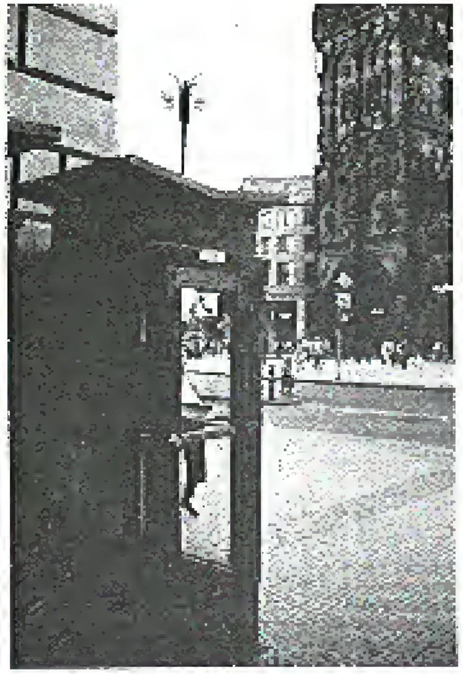
2600

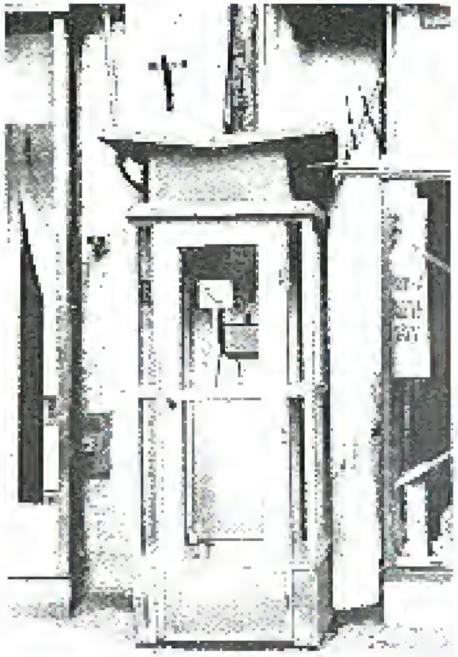
The Hacker Quarterly
VOLUME SIX, NUMBER FOUR
WINTER, 1989-90



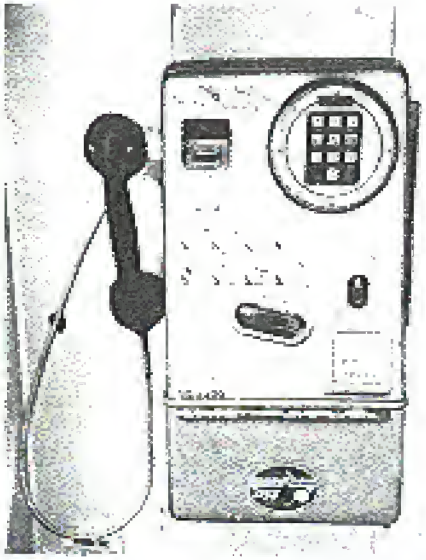
you talk of times of peace for all, And then prepare for war...
LET X≠Y

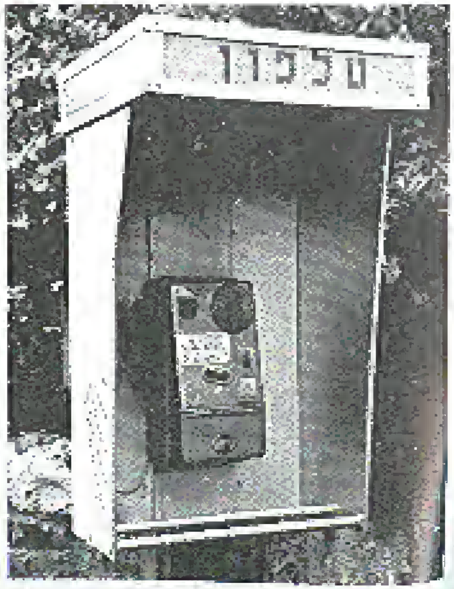
MORE COMMUNIST PAYPHONES
In Czechoslovakia





CAPITALIST PAYPHONES
In Israel

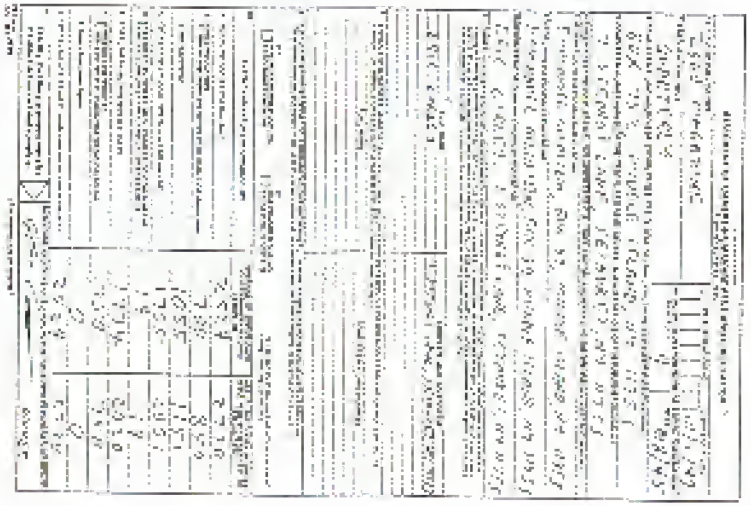




2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988
at $25 per year, $30 per year overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.

2600 Office Line: 516-751-2600, 2600 FAX Line: 516-751-2608



STAFF
Editor-In-Chief
Emmanuel Goldstein
Artwork
Holly Kaufman Spruch
Design
Zelda and the Right Thumb
Writers: Eric Corley, John Drake, Paul Estev, Mr. French, The Glitch, The Infidel, The Plague, David Ruderman, Bernie S., Lou Scannon, Silent Switchman, Violence, and the growing anonymous bunch.
Remote Observations: Geo. C. Tilyou

the day the phone system REALLY died

We all knew the day would come. And at least some of us were prepared for it. But, as usual, the vast majority had absolutely no idea what was going on.

AT&T was hit hard by a computer worm on January 15. That is a fact. And after reading the technical explanation below, you'll see why this is so.

But AT&T wasn't the only entity hit by this worm — we all were, some far more than others. The inability to get through, the denial of access, coupled with the blind faith we put in technology, the unwillingness to spread information so we can all *understand* the process. Yeah, it was fun for the phone phreaks as we watched the network crumble. But it was also an ominous sign of what's to come.

In the words of a high-ranking AT&T person, "very little could have gone worse". According to AT&T, of 148 million attempts, only 50 million went through. Many claim it was far worse than that.

> *"The news here isn't so much the failure of a computer program, but the failure of AT&T's entire structure."*

But what was it that actually happened? Here's what we were able to determine:

The problem started in a 4ESS machine in New York. The 4ESS is used to route calls and is basically, in the words of a Bell Lab technician, "nothing more than a big computer". New York, for reasons unknown, sent out a broadcast warning message (BWM), which triggered all of the 113 other 4ESS machines around the nation to do likewise.

Why did this happen now? Well, back in the late seventies, Bell Labs developed a common channel signalling system known as System Six or CCS 6. International standards have been developed over the past couple of years which necessitated some change on AT&T's part. So CCS 7, or System Seven, was introduced. Somewhere inside System Seven is where the problem lurked, undetected, until January 15.

According to experts, System Seven is a much more flexible system and that's why it's become the international standard. It's actually more of a protocol to which each company must adjust. They don't all use the same software. AT&T uses its own software, British Telecom uses something different, U.S. Sprint uses something else, etc. Some AT&T people, aided by well-meaning but ignorant media, were spreading the notion that many companies had the same software and therefore could face the same problem someday. Wrong. This was entirely an AT&T software deficiency. Of course, other companies could face completely *different* software problems. But, then, so too could AT&T.

The 114 4ESS machines around the country have new software installed periodically. When this is done, it's done gradually, circuit by circuit, one machine at a time. The network is presently configured so that the 4ESS machines have some circuits consisting of both System Six and System Seven. Eventually, though, all ties to the Six will be eliminated. "There's no reason to be concerned with this," AT&T says. "We've had some major changes in the network in the last ten years. In fact, we've had quite a few in the last three or four. They've always been for the better."

But what caused the problem? Exactly the right situation occurred at the right moment for a particular event to occur. Possibly the fact that January 15th was a holiday had something to do with it. Traffic was fairly low, which was unusual for a Monday. It's assumed that the problem originated in a particular component known as Common Network Interface (CNI) Ring. There is a component of that ring that allows the 4ESS to transmit messages across the ring and across the Common Channel Signalling Network. What apparently happened was that there was a flaw of some kind in the software in one of those rings. The bogus BWM from New York was sent out and it caused an excess of messages going to other 4ESS locations. A snowball effect began and the congestion spread and grew rapidly. All of the 4ESS machines were effected within half an hour.

Sounds like a worm to us. Not the kind that gets spread deliberately. There are plenty of programming errors that cause accidental worms. It could happen to any computer system.

Phone calls were forced off of System Seven and onto System Six. The problem was fixed by overwriting part of the software, in effect, bypassing it. But, at press time, the specific cause still hadn't been made known.

The name of the organization of Bell Labs software people trying to figure all of this out is NESAC, National Electronic Switching Assistance Center. They're working out of Lyle and Indian Hill, Illinois.

Lack of Redundancy

One expert said, "There's been a tendency in this company to save money by centralizing operations and making things bigger. And that has made the whole system more vulnerable."

There is much less redundancy in today's system, meaning there is less of a backup. The current infatuation with fiber optics that certain long distance companies have (AT&T included) spells certain trouble because of the lack of redundancy in these cheap systems.

The problem occurred in a part of the signalling system that doesn't carry voice traffic. It's known as "out-of-band signalling" because it's outside the band that carries the actual conversation. Data, such as the number called and the number calling, is sent over this path. Among other things, this prevents blue boxing since subscribers have no access to the routing signals.

And that's basically all we know at this stage. What we don't know is how a major force in communications like AT&T could be so sloppy. What happened to backups? Sure, computer systems go down all the time, but people making phone calls are not the same as people logging onto computers. We must make that distinction. It's not acceptable for the phone system or any other essential service to "go down". If we continue to trust technology without understanding it, we can look forward to many variations on this theme.

AT&T owes it to its customers to be prepared to *instantly* switch to another

(continued on page 45)

our ever-changing world

Morris Found Guilty

Robert T. Morris Jr., the 25-year-old Cornell student responsible for the Internet Worm, was found guilty on January 22 of federal computer tampering charges in Syracuse, NY. He now faces five years in prison and a $250,000 fine. He was the first person to be prosecuted under a portion of the 1986 Computer Fraud and Abuse Act. A hearing is set for February 27 in Albany, NY. Sentencing will probably be scheduled then.

The government argued that Morris intentionally wrote the worm program to break into "federal interest" computers he was not authorized to use, and by doing this prevented their authorized use and caused a minimum of $1,000 in damage.

Several jurors said it was obvious Morris didn't intend to do damage. But they say the damage would never have happened if Morris hadn't put the worm there. None of the jurors owned a home computer.

One juror said of Morris, "I believe his integrity. I did not believe there was any malice intended."

Another said Morris was "not a criminal. I don't think he should go to jail. I don't think jail would do anything for him. To me jail is for criminals, and he's not a criminal. I think somebody should thank him in the end."

In its November 26, 1988 edition shortly after the Internet Worm made its appearance, the New York Times described Morris as "fascinated with powerful computers and obsessed with the universe created by interconnected networks of machines".

Last year Senator Patrick Leahy of Vermont said, "We cannot unduly inhibit that inquisitive 13-year-old, who, if left to experiment today, may, tomorrow, develop the telecommunications or computer technology to lead the United States into the 21st century." He also expressed doubts that a computer virus law of any kind would be effective.

There is no doubt that Robert Morris Jr. has a lot of potential. There seems to be no doubt that he's an honest person. Even the prosecution seems to believe this. We all know that he was the person responsible for the Internet Worm. So, with all of this in mind, it seems as if the last few weeks have been a tremendous waste of time for everyone.

Yes, he did it. He admitted doing it. He didn't mean to cause damage, but he made a programming error. The shocking fact is that one programming error could cause so much confusion. Add to that the fact that the holes he made use of were common knowledge to the Internet community. Yet, nothing was done to close the holes until after all of this happened. It seems like someone should answer for this neglect of responsibilities. And let's not forget one other important fact. Morris never logged into another computer system without authorization. There is no proof that he ever planned to. He simply sent out a program to collect data — through normal and legal channels. It was data he never should have had access to, but thanks to the holes in the system, he did.

Morris made a mistake. That's all a part of the learning game, which he's now been banished from. This technology is still in its infancy and, like any system, its limits need to be constantly tested. We're making a very grave error if we choose to simply focus upon the debatable legalities of what he did, rather than learn from what he's taught us.

We're damn lucky it was Morris who did this. Because if a malicious or immature person had done it first, the damage would have been real.

Real Damage

A rather nasty "trojan horse virus" has been showing up on floppy disks throughout Europe, Africa, and California. More than 10,000 floppy disks labeled "AIDS Information Introductory Diskette" have turned up. After a random number of times, the program will format the hard drive and destroy all data on it. PC Business World Magazine says its mailing list had been used by the unknown creators of this mischief. They're offering a free program called "AIDSOUT" to anyone who was hurt by the diskette. If nothing else, this incident may remind people that running unknown software in this day and age is a risky thing to do. It's estimated that the cost of putting this whole prank together was about $20,000 which is a crime in itself.

Jailed for Incompetence?

A Georgia man is facing up to 15 years in jail for illegally accessing a computer. He was convicted in November. The difference here is that the defendant claimed innocence because of technical ignorance. Legal experts say this could be a trend-setting case, where users could become legal scapegoats for system crashes.

New Technology

Imagine a day when you can use any calling card number (AT&T, Sprint, MCI, and all the others) to make local calls as well as long distance ones. Imagine a day when

news and happenings

the Sprint operator will actually accept a Sprint calling card! Imagine not being confused. It all could happen as Bellcore develops a new, though temporary, system for handling calling cards. The plan calls for 14 digit credit card numbers. The first six digits would be known as the Card Issuer Identifier (CIID). That would be different for every company. The next four digits would be the customer account number and the last four would be a personal identification number. The plan is being developed as a quick and temporary way of allowing alternate long distance companies to use calling cards to process local calls. The whole thing will be reevaluated in 1991. One problem we find is the shortness of the customer account code (four digits?!). Why is the company given six digits? Are there a million companies? Perhaps they're not explaining this properly. It wouldn't be the first time....

And Things To Play With

New York Telephone has a new toy that allows them to fire even more employees. Now, when you dial zero plus a number and hit another zero at the tone, you get a computerized menu, which says, "For collect calls, dial 11; to charge this call to another number, dial the complete billing number now; for person-to-person and other calls, dial 0 for the operator." When you dial 11, you're asked to record your name. The advantage here is that your name can be anything you want, like "Call Me Back". The system uses voice recognition when asking the called party if they accept. The caller's mouthpiece is cut off during this procedure, so you can forget about accepting your own call. Also, the system won't accept a response that begins before it finishes asking the question. This helps eliminate answering machines that may inadvertently say "yes" at some point. Third party billing is only verified when you place the call from a payphone. The system asks you for your name at that point. It's fun to play with, but once again, ultimately a ripoff for the average consumer. The rates haven't gone down, even though it's pretty obvious that this system will save New York Telephone a bundle. But the worst part of all is for those people who have resisted getting a touch tone phone (and paying the unfair monthly and "installation" fees). Instead of getting an operator a couple of seconds after the initial tone, pulse customers must sit through the entire menu before the system finally connects them to an operator. The waiting time for an operator under the old system: three seconds after

(continued on page 42)

nynex data

by The Plague

(Special thanks to Kornflake Killer)

The following information and data relates to the NYNEX (New York & New England Telephone) telephone switching system. Most of the article is a huge database of New York Telephone centers further subdivided by sector. It contains useful information on every switch in the NYNEX system. This information is very handy in social engineering, plotting network switching maps, and finding out particularly useful information about your Central Office. There is usually more than one switch per central office. Since step-by-step offices tend to be good for blue boxing, this information could come in handy.

In the database the following fields exist:

SECTOR - this is Nynex terminology for a large inter-office and billing center (i.e., Williamsburg or White Plains). All switches throughout NYNEX are connected to one of these main centers.

The following New York sectors are established by NYNEX:

(Sector:Switching Type:Location)

ALBY:D200:Albany BING:1AESS:Binghamton
BUFF:D200:Buffalo CISP:4ESS:Central Islip
GDCY:4ESS:Garden City NY21:4ESS:Soho
NY38:4ESS:East 38th St POUG:5ESS:Poughkeepsie
SYRA:D200:Syracuse WHPL:4ESS:White Plains
WLMG:4ESS:Williamsburg

CLLI code - Common Language Location Identification. This is Bell system shorthand for the location and type of the switch. You can refer to Bell Labs and Bellcore literature or the October 1987 issue of 2600 for more details. A CLLI code consists of 11 characters. The first 4 characters define the town, the next 2 characters define the state abbreviation, the next 2 the building ID, and the last 3 the building subdivision.

Example: NYCMNY42CG1 is New York City Manhattan, NY, 42nd street, Control Group 1 (representing a 1, 1A, 2, 2B, or 2ESS switch).

SWITCH TYPE - The switch type, can be one of the following: AESS, 1ESS, 1SXS, 2BESS, 350ASXS, 3556ASXS, 355ASXS, 356ASXS, 360ASXS, 2ESS, 5XB, D10, D100, DSF, NCXB, RSM, RSS. (XB = Crossbar, ESS = Electronic Switching System, SXS - Step by Step, D = DMS/Digital, R = Remote)

V & H - These are numbers used by Bell Companies to represent Vertical and Horizontal location. These are integers which are offsets from a fixed point on the earth designated by the phone company. These numbers are used in calculating distances between central offices as well as for network planning. Any entries in the following databases which have the same V & H are in the same building/location. You should read Bell Labs and Bellcore literature to find out more about V & H and network planning.

HOST Switch - This field is shown only for those switches which are remote in nature (RSM and RSS). This field is simply the CLLI code of the host switch that connects to the remote switch.

This article should be used as reference material, and doesn't go into explaining any details about switching. Refer to other articles and Bell literature for that information.

You may need a magnifying glass to read all of this but it was the only way we could fit it in the issue. Fields are separated by the : symbol. If there is a HOST switch present, it appears on the following line indented.

```
New York Telephone
Sect:CLLI Code:Sw Typ:V:H:
    Host Switch
[illegible]
```

every central office in new york state

[illegible]

now you know

[illegible]

what they know

[illegible]

MORE HACKING ON PRIMOS

by Violence

This is the second part of a series on the PRIMOS operating system. In this part I will detail the several useful applications you are likely to find on Prime computers. You will learn about the DSM (Distributed System Management) utilities, the EDIT_PROFILE utility (the PRIMOS user editor), and several others. This will enable you to make the most of any Prime computer you happen to visit.

Examples appear in italics. Bold italics indicate user input, regular italics indicate computer output.

EDIT_PROFILE

EDIT_PROFILE is the utility that is used to add, delete, and modify users on a Prime computer running PRIMOS. It is similar to the VAX/VMS AUTHORIZE utility. There are three modes of EDIT_PROFILE access, and these are:

System Initialization (SI) mode
System Administrator (SA) mode
Project Administrator (PA) mode

You will probably never be using EDIT_PROFILE in System Initialization mode as that mode is used for initial system user setup. SA mode will allow you to perform wholesale user modifications, whereas PA mode will only allow you to perform modifications to users in the same project as you. When you decided to try out EDIT_PROFILE on the system that you have hacked into, type this:

```
OK, edit_profile
```

If it gives you an error message then you obviously don't have good enough privileges. Don't give up hope, however, as there are ways around this. Unfortunately, though, the methods which you must use are beyond the scope of this tutorial. It involves programming in a high level language (FORTRAN IV, FORTRAN-77, PL/1 Subset G, et. al.) as well as knowledge of the appropriate system calls to make. Do lots of research and experiment. You might just get lucky.

If, on the other hand, it allows you to invoke EDIT_PROFILE then it will display the utility's herald (revision number, serial number, and copyright information) and a message stating what mode you are in. The mode message will be one of these:

```
In system administrator mode
In project administrator mode
```

If you are in SA mode then the account you are using has SYS1 privileges (that's the best you can do from a remote standpoint). Before I get deep in how to use EDIT_PROFILE properly I should mention that I have the source code to this wonderfully useful program and a security audit feature was added in during the last few years (circa 1986). It will log all successful and failed commands. The only way I have discovered around this is to remove the logging procedures from the code and recompile it online, but that's pretty advanced stuff and not advised at any rate. The best you can do at maintaining your presence on the system is not to use EDIT_PROFILE overly much. In fact, don't use it unless you must. I generally use EDIT_PROFILE once per hack, and that is after I get in. What do I do? I obtain a full user/project listing for future hacking purposes. You can't obtain an account's password from within EDIT_PROFILE, but you can obtain a full user and project listing, as well as add, modify, and delete users. If you get a user list, try and hack at those accounts before wantonly adding user accounts. Be sensible. Get all that you can before adding a user. And if you must add a user, just add one. There is no need to add three or four users. No need at all. One user is easier to hide than three or more. Use common sense here, guys.

"One user is easier to hide than three or more."

Once EDIT_PROFILE has been invoked you will be dispatched mercilessly to the ">" prompt. To obtain help, just type HELP and press RETURN. Before I get into adding users, I'll discuss the procedures for pulling user lists and similar information.

To get full information about the system you are on (projects, users, etc) you simply need to type:

```
>list_system -all
```

You can abbreviate the LIST_SYSTEM command with LS. You can list individual system attributes by substituting new arguments in place of the -ALL argument. To see what LS arguments are available, type HELP. You should experiment with the available "LIST_" commands in EDIT_PROFILE

Before attempting to add a user on any Prime system you should always list the system attributes so that you will know what projects and groups are in use. When you decide to add a super-user, make sure that you add yourself to the common project (usually DEFAULT) and all of the high-access groups (examples I have seen are: .ADMINISTRATORS$, .PROJECT_ADMINISTRATORS$, .OPERATORS$, .NET_MGT$, etc). Adding super-users is not always a good idea. Never add more than 1 or 2 users on a system. Also, try to follow the naming conventions used on the system. If users have their first name as a User ID, then when you add a user make sure that your new user's User ID is a first name. Likewise, if all users have their initials as their User ID then make sure that your new user has a User ID with initials. Now, to add a user, type:

```
>add_user username
```

Where "username" is the User ID you wish to use. After you type this you will be asked for your password. Enter the password that you wish to use. Then you will be asked for your group(s) and your default login project. Like I said, you should use the "LIST_" commands to see what group(s) are in use. Groups always start with a period (.). Give yourself the administrator groups and you will be doing good. As for project, an entry of DEFAULT will usually suffice.

An easier method to add users is to use the -LIKE argument. Try this

```
>add_user username -like system
```

Again, "username" is the name of the User ID that you wish to use. This argument of the ADD_USER command will make a copy of the user called SYSTEM (found on all Primes that I have seen; also a user of the super-user class) and add the copy as a new user but with a different name. Now, set your password with the CHANGE_USER command. Type:

```
>change_user username -pw
```

You will be prompted for your new password. Ta da. You now have a User ID with the same stats as the User ID "SYSTEM". Occasionally upon adding a user you may have to add your User ID to a file called LOGUFD located in one of the UFD's off of MFD 0. This will generally not happen. If it does, then simply correct it with one of your other accounts.

You are advised not to wantonly delete users or edit them. Also try not to use the CHANGE_SYSTEM _ADMINISTRATOR command. Basically, type HELP and start to experiment (but be careful of what you do). Make sure that you keep track of the changes that you make so that in case you mess something up you can fix it. Get your feet wet.

If you find yourself in PA mode you can do most of the above, but only regarding the project that you are administrating. Thus you can only add users to that project, only delete users from that project, etc. This means no adding of super-users, etc.

The Distributed System Management (DSM) Utilities

The DSM utilities is a set of commands and services that help with the administration and day-to-day operation of Prime computer systems. It is intended primarily for use with networked systems, but can also be used on single Prime systems (those lacking networking capability).

The DSM utilities allow Prime system administrators and senior operators to perform system management tasks from any point on a network. DSM's main facilities

MORE PRIME HACKING

are summarized below.
SIM (System Information/Metering) Commands System status and resource monitoring of local and remote systems from any point within the network.
RESUS (REmote System USer) Facility Control of remote Prime systems from any terminal. Allows use of console-only commands from a remote terminal.
Collection and collation of event messages, including PRIMOS and network events, through DSM's Unsolicited Message Handling (UMH) and logging services, with redirection of event messages to log files or users throughout the network.
Generalized logging of DSM messages in private or system logs, with commands for administering, displaying and printing logs.
Facilities for defining users' access to DSM commands throughout the network, in a single configuration file.

As you can see, the DSM utilities can be a very useful asset to have. Unfortunately, SYS1 privileges (administrator) are required to use the most exciting aspects of the DSM utilities. All normal users can utilize the SIM commands, and I have even mentioned some of them in other parts of this series. What is really useful to us, however, are the RESUS and log utilities. In a nutshell here are the basic DSM commands. After this list will be full discourses on the RESUS utility and the SIM commands.

Remote System Control:
RESUS — Invokes Prime's REmote System USer facility.
Event Message Handling and Redirection:
CONFIG_UM — configures DSM Unsolicited Message Handling.
Administering Logs:
ADMIN_LOG — creates and administers DSM log files.
Displaying and Printing Logs:
DISPLAY_LOG — displays and prints the contents of log files, including system and network event logs.
DSM Configurator Commands:
CONFIG_DSM — creates a new DSM configuration file.
DISTRIBUTE_DSM — distributes a new DSM configuration file.
STATUS_DSM — displays the currently active configuration.
DSM Startup and Shutdown Commands:
START_DSM — starts DSM system console commands.
STOP_DSM — stops DSM system console commands.

For more information on any of the DSM commands, type:
HELP command-name
or
command-name -HELP

The RESUS Utility

RESUS is the REmote System USer facility, and allows remote operation of the physical supervisor console from any terminal. What this basically means is that, with RESUS enabled, all users with administrator access will be able to execute commands that are normally only executable from the system console. It will let you force other users off the system (not a good idea to use this capability unless you MUST), take the system down (you must be STUPID to do such a thing), etc. RESUS supports the following command line options:

-ENABLE
-DISABLE [-FORCE]
-START [-ON node name]
-STOP
-STATUS [-ON node group]
-HELP [-NO_WAIT]
-USAGE

-ENABLE

This option enables RESUS to be used on a system. It is only valid from the supervisor terminal.

-DISABLE

This option is used to prevent RESUS from being used on a system on which it has previously been -ENABLEd. The -FORCE option must be supplied if the RESUS is actually in use. It is only valid from the supervisor terminal.

-START [-ON node name]

This is the means by which an authorized user of RESUS may invoke REmote System USer facilities on a system. If -ON node name is omitted, the default is the local node. For this command to be successful, RESUS must previously have been -ENABLEd at the supervisor terminal.

-STOP

This option terminates remote control of the supervisor terminal, leaving the REmote System USer facilities available for use by other authorized users. It is only valid from the remote terminal in control of the supervisor terminal through RESUS.

-STATUS [-ON nodegroup]

This displays the current status of RESUS on all nodes in a specified node group. If a node group is not specified, the status of the local node is displayed.

-HELP, -H [-NO_WAIT, -NW]

Displays command-specific Help text.

-USAGE

Displays command line syntax.

The DSM SIM Commands

The DSM SIM (System Information/Metering) commands gather and display information about system/network status and resource usage from any point on the network.

SIM commands are invoked from the PRIMOS command line. They can be invoked from any terminal to display information about any system on the network. They can be invoked once, or periodically at specified time intervals. Output displays are paginated for screen display and can be recorded in private or system log files. User access to SIM commands on local and remote nodes is controlled by DSM security.

A list of SIM commands and descriptions of the general SIM options follows.
LIST_ASSIGNED_DEVICES - lists assigned devices
LIST_ASYNC - lists asynchronous terminals
LIST_COMM_CONTROLLERS - lists comms controllers configuration
LIST_CONFIG - lists PRIMOS coldstart configuration
LIST_DISKS - lists disk partition names
LIST_LAN_NODES - lists nodes on LAN300 local networks
LIST_MEMORY - lists physical memory usage
LIST_PRIMENET_NODES - lists PRIMENET configured nodes
LIST_PRIMENET_LINKS - lists active PRIMENET links
LIST_PRIMENET_PORTS - lists assigned PRIMENET ports
LIST_PROCESS - lists active system processes
LIST_SEMAPHORES - lists active semaphores
LIST_SYNC - lists synchronous line configuration
LIST_UNITS - lists users open file units
LIST_VCS - lists active virtual circuits

General SIM options are:
-HELP, -H [-NO_WAIT, -NW]
-USAGE
-ON {node, nodegroup}
-PRIVATE_LOG, -PLOG pathname [-NTTY, -N]
-SYSTEM_LOG, -SLOG pathname [-NTTY, -N]
-NO_WAIT, -NW
-FREQ integer
-TIMES integer
-START, -S date+time
-STOP date+time

-ON {node, nodegroup}

This option allows you to specify the target node, or nodegroup to which the command is to be directed. The default is to direct the command to the node on which the command is invoked.
-PRIVATE_LOG, -PLOG pathname [-NTTY, -N]
-SYSTEM_LOG, -SLOG pathname [-NTTY, -N]

The -PRIVATE_LOG option allows you to specify a standard PRIMOS pathname as a DSM log file to which all messages from the target nodes are to be logged. If the log does not already exist, it is created automatically for you. User DSMASR (the DSM application server) must have ALL access to the directory that contains the log.

The -SYSTEM_LOG option allows you a similar facility using logs that are maintained on the system logging directory DSM*>LOGS. System logs only exist on

INFILTRATING A PRIME

this directory or its subdirectories, and must be created with the ADMIN_LOG command prior to use.

Logged data can subsequently be retrieved, printed and displayed using the DISPLAY_LOG command.

-NTTY, -N, can be used with the -PRIVATE_LOG and -SYSTEM_LOG options, and indicates that no data is to be displayed to the user. When this option is used, the command spawns a phantom which executes the command on your behalf, and frees your terminal.

-HELP, -H [NO_WAIT, -NW]

This option overrides all other options to display help information about the associated command.

-USAGE

This option overrides all other options to display usage information, for the associated command.

-NO_WAIT, -NW

This option indicates that you are not to be prompted or queried during the command output display.

If this option is not used, you are prompted between each target node's response, and after every 23 lines (1 page) of output displays "—More—" and waits for your response. To see more output press the carriage return. To suppress further output and return to command level, type Q, Quit, N, or No. Any other response will display more output.

-FREQ
-TIMES
-START, -S
-STOP

These options can be used to implement periodic execution of a command.

-FREQ option provides periodic execution of a command, with the interval between executions determined in seconds. The interval you specify is the interval between two successive executions of a command, and not the interval between completion of the command's display and the next execution. The interval is corrected to the nearest multiple of four seconds below that specified. If FREQ 0 is specified, the command is re-executed immediately on completion of the previous execution. If the interval elapses before completion of the previous display, the next execution is delayed until the display is complete.

-TIMES is used in association with the -FREQ option, to set a limit on the number of times that a command is to be executed.

-START, -S sets the date and time that execution starts. The format can be in either ISO standard.

(YY_MM_DD.HH:MM:SS)

or in USA standard.

(MM/DD/YY.HH:MM:SS)

Defaults are: year to current year; date to current date; and time to zero.

-STOP sets the date and time execution stops; format and defaults are the same as for -START.

In the absence of any of these four options, the command is executed once, and immediately.

In the presence of any of these four options, the defaults applied to the unspecified options are:

-FREQ - Immediate reexecution
-TIMES - Infinite
-START - now
-STOP - never

For more information on any of the SIV commands, type:

HELP command-name

or

command-name -HELP

PRIMOS Electronic Mail Capabilities

PRIMOS, like any other operating system worth its beans, supports full electronic mail capabilities. However, the mail system used will vary from system to system. A lack of standards? Perhaps. But I find it enjoyable learning the differences between the many mail systems available.

I won't discuss how to use the mail systems due to lack of space, but that should pose no problem, as all of them have online help available.

Prime Computer, Inc.'s old mail system (invoked by typing MAIL) is your typical run-of-the-mill mail system. It's not too difficult to figure out how to use.

Prime Computer, Inc. has also created a PRIMOS implementation of the UNIX XMAIL system. This seems to be their preferred electronic mail system. It is very easy to use, not to mention very powerful.

My favorite electronic mail server is NETMAIL, written by those cunning programmers at Bramalea Software Systems (the same firm that created LOGIN_SENTRY). NETMAIL is the mail server with the most useful features. Not only do you get the normal features of sending user-to-user mail locally and to similarly configured sites on the network, you can also send:

Courtesy copies to other users
Encapsulated non-SAM files

Courtesy copies is basically message forwarding. Assume I wrote a memorandum. If I wanted all the people on the "Board of Trustees" to get a copy I just send cc's (courtesy copies) to them.

The file encapsulation feature makes NETMAIL a pseudo-file transfer application like FTS (File Transfer Service, Prime's answer to UNIX's FTP utility). Say I wrote a useful public domain program and want to distribute it to some users on the local system and some remote systems. Don't want them to get the sources, now do we? So we encapsulate the executable file (compiled program) and mail it out as an encapsulated file. When the receivers read their mail, they will be able to tell NETMAIL to save it as a file to their directory. Very nice!

Some sites use custom-written mail utilities. It all depends. Most, if not all, are rather user friendly and easy to learn without documentation. Don't forget! Online help files.

ED - The PRIMOS Text Editor

ED is the PRIMOS text editor and it is line-oriented as opposed to full-screen. If you are using VT-100 or a similar emulation, you might play around with the EMACS full-screen editor, but I won't be discussing EMACS here. After all, it comes with its own interactive tutorial. Another reason why I won't be discussing it is because not all Prime sites have it online (it is a separately priced product). RUNOFF is another separately priced product. It is a fully equipped word processor. ED, on the other hand, comes with PRIMOS and it is always available.

To invoke the PRIMOS EDitor, type:

ed

at the "OK," prompt.

This will enter ED with an empty workspace. You are creating a new file. To edit an existing filesystem object, type:

ed filename

When you enter ED with an empty workspace you will be dumped into INPUT mode. Everything you type here will be taken as input into the file you are creating.

If you tell ED to load a file and edit it (i.e., ED filename) then you will be dumped into EDIT mode. Everything you type will be taken as ED editing commands.

To switch between INPUT and EDIT mode, issue a null line (that is to say, press the RETURN key). This brings a new problem into mind. How do you make a blank line if when you press RETURN alone it switches between modes? Yes, this is a shortcoming for PRIMOS users who are used to standard text editing systems. To create a "null" line, type a space and then press RETURN. It looks null, but it is really treated as a line one character in length by ED. Take note that both INPUT mode and EDIT mode use no prompt.

> *"You are advised not to wantonly delete users or edit them."*

To illustrate what we have learned so far, consider this "pretend" session with the ED line editor. *(Since this magazine is not an 80 column environment, we'll use the ">" symbol at the beginning of lines that are actually part of the preceding line in an 80-column setting.)*

```
OK, ed
INPUT
Hey, this is pretty nice. A nice text
```

(continued on page 34)

HOW TO BUILD A SILVER BOX

by Mr. Upsetter

Every day people use touch tones to signal between their phone and the phone company's switching equipment. What the average man on the street doesn't know is that there are four other touch tones that aren't used in regular telephone signaling. As all good phone experimenters know, a silver box is a device that can create the four extra DTMF (dual-tone multi-frequency) tones that are not used in normal telephone service. These DTMF tones are known as A, B, C, and D. It is quite easy to generate these DTMF tones because the standard 16 tone format is used in many popular DTMF tone generator IC's. This article shows two ways to modify telephone equipment on the market to make silver box tones and then gives a schematic of a device that will produce all 16 DTMF tones.

Modification for Telephones

You may not know it, but you might already own a silver box. That is, the DTMF encoder IC inside your touch tone phone may be capable of producing silver box tones. If your phone is a newer touch tone and does not have features such as call storage or redial, the mod presented here will work, if it has the right chip.

There are many different types of DTMF chips, but this modification is for phones using the 16 pin TCM5087 tone encoder. This chip is specifically designed to generate the eight different tones used in dual tone telephone dialing systems. See Figures 1 and 2 for a list of tones and associated frequencies. Here's how the 5087 works. When a key is pressed, it connects two pins on the IC together. One is a row pin and one is a column pin. For instance, if a 6 is pressed, the row 2 pin is connected to the column 3 pin on the 5087. This causes a 770 Hz and 1477 Hz tone to be emitted. For normal phone use, the column 4 pin, which is used to make the A, B, C, and D tones is unused.

Before you start this simple modification you must have a phone with a 5087 chip. On the new trimline style phones this chip is located in the center of the larger printed circuit board (PCB) in the handset. The chip should have the numbers 5087 on the back along with some other numbers, so it will read something like "T95087" or "TCM5087". Once you have identified the chip, you must gain access to the solder side of the PCB.

The four tones are enabled by installing three wires and a switch. First, cut the trace on the PCB going from pin 5 of the 5087 to the keypad. Use a razor blade or a small file. (On an IC the first pin is the one in the lower left corner when you hold the chip so the letters are right side up. There may also be a dot on the case above pin 1.) Next, solder separate wires to pin 5, pin 9, and to column 3 of the keypad. This is the point on the keypad that was connected to pin 5 of the IC before you cut the trace. See Figure 3 for the schematic of the modification. On a trimline type phone it is easiest to make all connections to the solder side of the PCB. Be sure you have identified the pins on the IC correctly before you start soldering. Now, solder the wire from the keypad to the middle tab of an SPDT switch. Solder the wire from pin 9 to one side of the switch and the wire from pin 5 to the other. The modification is now complete. For normal DTMF tones the switch simply connects the keypad to pin 5, the column 3 pin. For silver box tones, the switch connects the previously unused pin 9, the column 4 pin, to the keypad. The keys 3, 6, 9, and # now become A, B, C, and D respectively.

Before you put everything back together doublecheck your work. Toggle the switch and make sure all the tones work. Make sure the wires you installed don't cause any shorts. Lastly, find a place to securely install the switch.

Another Modification

If the above mod won't work on any of your phones, you can do a similar mod on a product sold by Radio Shack. Their "economy pocket tone dialer" ($15.95) uses a 5087 chip and can be converted for silver box tones. The modification uses three wires and a switch, as before. Once completed, you will have a nice portable 16 tone DTMF generator.

The first step of this mod is to remove the PCB. Carefully pop off the back of the unit and remove the power switch and the six screws in the PCB. Then desolder the two speaker wires and the battery wires from the PCB. You may also want to remove the keypad and the keys. Now look at the keypad side of the PCB (not the component side). Cut the trace going from pin 5 of the IC to column 3 of the keypad. This is the outermost of the three traces going from the IC to the keypad. Now the switch must be installed. Find a tinned round pad marked C3 in the upper left of the component side of the PCB and solder a wire from here to the middle tab of an SPDT switch. This switch must be a very small toggle or slide switch. Also on the component side, solder a wire from pin 9 to one side of the switch and a wire from pin 5 to the other. As before, be sure to identify the pins correctly. There is room to install a switch inside the enclosure in the gap to the left of the diode at the top of the PCB. As usual, check for shorts caused by the wires or the switch. The switch will operate exactly as described in the previous modification.

Alternative 16 Tone DTMF Generator

If you don't have the right phone and don't want to spend $16 at Radio Shack, you can build your own touch tone encoder using the schematic in Figure 4. This device is very similar to the one sold by Radio Shack. It uses the TCM5089 DTMF encoder IC to produce all 16

USING THOSE FOUR EXTRA TONES

tones. The 5089 is closely related to the 5087 in both function and pinout. One important difference is that the 5087 produces a tone when a row and column pin are connected together, while the 5089 produces a tone when a row and column pin are connected to ground. As a result, the 5089 must be used with a specific type of keypad, called a 2-of-8 keypad.

Explanation of the schematic is as follows: pressing a key causes a row and column pin to go low, thus producing a DTMF tone at pin 16, the output. The IC requires a sine wave input supplied by a TV color-burst crystal at 3.579545 MHz (X1) to generate eight different audio sinusoidal frequencies. The tone output from pin 16 goes to a 32 ohm speaker, C2, C3, and R1. Varying the values of C2, C3, and R1 will change the volume and audio quality of the signal. If you use a speaker of higher and lower impedance, you should experiment with the values of C2, C3, and R1 for the best audio volume and quality. The device is powered by 4.5V but the 5089 can handle up to 12V.

Parts List and Suppliers

C1- 22uf, 16V electrolytic

C2- 1uf, 16V electrolytic

C3- 2.2uf, 16V electrolytic

IC1- TCM5089 DTMF encoder

R1- 68 ohm, 1/4W

X1- 3.579545 MHz color-burst crystal

Other parts: 2-of-8 keypad, speaker, batteries, battery holder, enclosure, power switch, circuit board, etc.

The TCM5089 is available from many sources. One is Jameco Electronics, 1355 Shoreway Road, Belmont, CA 94002. A 2-of-8 keypad is available from The Electronic Goldmine, P.O. Box 5408, Scottsdale, AZ 85261. The crystal is available from Radio Shack or Jameco, and many others. Total cost of electronic parts should be around $6-7.

If you buy the keypad from The Electronic Goldmine, the pinout is as follows:

o o o o o o o o o
E F G H J K L M N

These are the nine pins on the back of the keypad. E: ground, F: column 4, G: column 3, H: column 2, J: column 1, K: row 4, L: row 3, M: row 2, N: row 1.

Now What?

Some of you may be wondering what to do with your new toy. A silver box isn't a toll avoidance device like a blue or red box; it is another tool with which to explore the phone system. And that means you have to do the experimenting. Try beeping silver box tones into voice message systems, cellular VMS, test exchanges, loops, pay phones, 10NXX and 950 numbers, answering machines, or anywhere else you think the tones shouldn't belong. See what happens when you drop a silver box tone or two down your local exchange or through different long distance carriers. If you experiment systematically and keep good records, you will surely uncover something interesting.

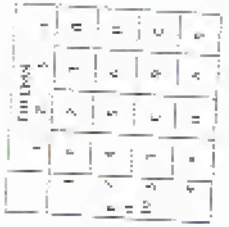


Figure 2

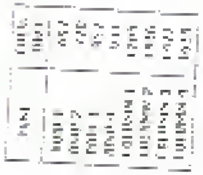

TONE	FREQ
ROW 1	697
ROW 2	770
ROW 3	852
ROW 4	941
COLUMN 1	1209
COLUMN 2	1336
COLUMN 3	1477
COLUMN 4	1633

Figure 1

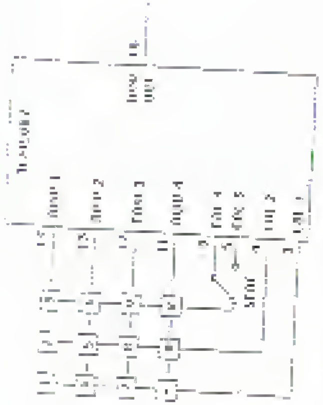
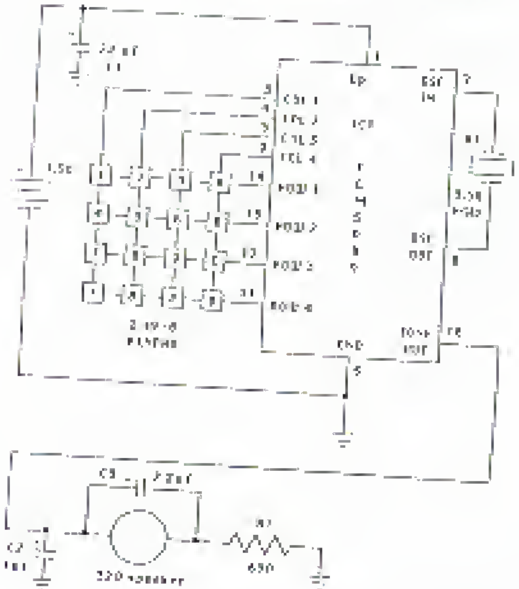


Figure 3. Note switch between pins 5 and 6

Figure 4. This schematic is similar to the Radio Shack device



words and characters

Help Needed

Dear 2600:

I am hoping you may be able to help me. I am in a position where several times people I do not know have tried to trick me into saying illegal things on the phone. I need a way to be able to tell their phone numbers as they call me.

I have heard that there exists phones or boxes that can pick up the number calling you from a signal transmitted with any call and display it. Do you know where I could buy one, get one, or how I could build one?

Concerned
Syracuse, NY

Yes, such boxes exist, but it will be some time before they can tell you the phone number of ANY call, that is, calls outside your local calling area. And it won't work at all if your local phone company isn't offering a caller-ID type of service.

Caller-ID is becoming a very controversial topic. Anonymity on the phone is something we all take for granted. Removing this would make using the phone a completely different experience, one that would probably be a whole lot less fun and a great deal more intimidating.

But then there are those who abuse the anonymity feature. What do we do with them? In your case, you'd be wise not to remain on the line when these people call if indeed they are trying to trick you. If they continue to call, file a complaint with your phone company. Nobody (including the phone company, law enforcement, or regular people) has the right to harass you on the phone if they're told to stop. If you're determined enough, they will be tracked down.

Interesting Facts

Dear 2600:

The ANI's for the 412 (Pittsburgh) area code are scattered in the 410 exchange. We know of the following:

410-4100: downtown Pittsburgh and suburban.

410-6633: east suburban.

Also, US Sprint issues a complete rundown of who called an 800 number. We got our 800 bill and surprisingly it showed every number that called us.

The Renegade of Pittsburgh
Sysop of Charlotte
(412) 829-2767

The copy of the bill you sent us looks exactly like a regular Sprint bill, except the numbers on it are the numbers that called you. Something to think about, especially those of you who like to call 800 numbers. Look in our Spring 1989 issue to find out which 800 exchanges are owned by Sprint. We'd like to know if the other companies provide such detailed billing.

By the way, Sprint's FONLine 800 service isn't a bad deal. There's currently no startup fee to obtain an 800 number and you can attach it to any existing phone number. Your 800 number will work all over the country and the monthly fee is only $10. The per call fee is rather steep, though. It averages about 22 cents a minute. But it's one way to virtually guarantee not getting ripped off by an AOS somewhere. Of course, you can only dial one number.

More Frequencies

Dear 2600:

In your Autumn 1989 issue a reader pointed out the Mobile Telephone Assignments. The reader however left out an important set of frequencies which are used for phones on airplanes. These frequencies usually have senators, congressmen, and other important business people calling home, setting appointments, or talking about other things:

454.675, 454.700, 454.725, 454.750, 454.775, 454.800, 454.825, 454.850, 454.875, 454.900, 454.925, 454.950, 454.975.

Please note: "It is a federal crime with severe punishment and/or fines to 1) divulge what you hear to anyone who is not a party to the broadcast; 2) to make use of any broadcast information for your own personal gain; 3) to make use of any broadcast information for illegal purposes or to commit a crime. Any such violations may be investigated by the FBI and prosecuted by the US Department of Justice."

MM
Rutherford, NJ

We wonder if those same penalties apply to anyone who overhears a conversation on a bus. It's basically the same thing. The only difference is that the people talking on the phone often aren't aware of how easy it is for others to listen in. The crime in that case is ignorance, often perpetuated by manufacturers who would rather their customers not know how non-private their conversations really are. Still, this is better than the cellular fiasco, where Congress decided that the best (and only) protection would be to simply make listening in illegal. Who would be fool enough to listen to something illegal in the privacy of their own home?

Numbers Needed

Dear 2600:

I am writing to inquire as to whether any issue of your magazine has information regarding access to long distance telephone calling card codes using AT&T or Sprint services without a computer.

I used to have a calling card number that worked and billed to someone else, but it is no longer valid.

I don't have a computer, so I need some way of finding a valid card number that works. From what I've read in one of your books, that isn't easy to do at random because AT&T is difficult to hack without a computer. I've tried using my old card and changing the last four digits, but it won't go through.

If you have anything on this or know of a publication that does, please let me know.

MC
Van Nuys, CA

What you want to do really has nothing to do with hacking or phreaking. There are lots of ways *to make telephone calls. You discover them through individual experimentation. Using someone else's calling card is not the way to go. You victimize an innocent person and you also run a tremendous risk of getting caught. If you want to explore and manipulate the system, there's never been a better time. If you simply want to steal, you'll have to wait in line.*

BBS Question

Dear 2600:

What are the requirements for putting up a 2600 BBS? I have an Amiga and I want to put up a board. What BBS program should I use?

Greg
New York

As it stands right now, there are no 2600 boards. It was working out fairly well for a while but then we found ourselves devoting more and more time to the boards when we should have been working on the magazine. We've got our priorities and they center around the magazine itself. Anyone interested in running boards has our blessings, and if they want to spread the word through 2600, we'll do what we can. The only basic requirements we insist upon are user anonymity and private mail that cannot be read by system operators.

Comments/ Suggestions

Dear 2600:

I had not intended to renew this time, since I've found very little of interest in the last few issues. In particular, the articles about the command languages of several (common) operating systems seemed no more than a reprint of what was easily available in users' manuals. I read those all day. Your Fall issue was superb, however, so I'd like to renew.

Don't misunderstand. I do like the articles on computers when they present something fresh. But, in general, I find the articles on the telephone system much more interesting. And I especially like the information on threats to privacy (and would appreciate more about "practical" ways to counteract these threats).

I do have one question. In many cases, the telephone information is a bit too advanced for me, as I am only a beginner. I would appreciate it if sometime you could publish a bibliography of above- and underground information, from which I could learn the basics. As you may have most of this information already, which may otherwise be hard to find, maybe you could put it altogether into a "primer" which you could offer for sale.

In closing, again, thanks for the last issue, which was golden.

RC
Phoenix

It WAS a good issue, wasn't it? We were responding to our readers' suggestions, which we never tire of hearing. We need a continuing flow of more articles, however, in order to keep issues like that one coming.

The project you suggest is one we've had our eye on for some time. We've had our eye on others as well. Maybe something will materialize soon...

COCOT Hacking

Dear 2600:

A non Bell System lookalike payphone was recently installed outside in the parking lot of a convenience store across the street from my residence. The phone wires coming out of it are exposed and unprotected; you could probably splice into them leaving extra connections to hook up a conventional telephone.

No phone number is listed on it so I made a short long distance collect call to a friend. A choppy woman's digitized computer voice said, "This is a public payphone. This is not a billable number." It repeated this about four or five times as the call was being initiated — even the person I phoned could hear it. I was then able to get the payphone's number from my friend's phone bill.

I called the payphone and after two rings the same voice answered by just saying "Thank you" followed by a series of four touchtones (I assume) in rapid succession. There's about a 20 second pause. (I would guess the payphone owners enter a code from a touchtone phone on their end to determine how much money has been collected, etc. It would be fun to hang an FM transmitter on the line and eventually get all the codes to activate its various information modes.) Without entering a chain of touchtones it recognizes, it simply hangs up.

I then took my cordless phone over to it and dialed it up. The payphone produces a soft chirping sound instead of a ringing bell, and it's not loud at all. When you pick up the handset it simply says "One moment please" four or five times but it simply will not connect you through to the caller. As a general rule I avoid these privately owned payphones and whenever possible go for genuine Bell.

As an open suggestion, could a knowledgeable 2600 reader submit a schematic for a device that would display a digital readout of a string of touchtones applied to its input? The NSA uses such devices in their surveillance work. Recently Modern Electronics had a device that would give an actual voice of the various touchtone digits. Its construction was fairly simple, but the tones had to be entered very slowly — it couldn't tell you a rapid string like you'd get from an auto speed dialer or even from normal hand dialing. This device would be great for monitoring cellulars or the 46/49 Mhz cordless portaphones.

And finally, one question: is it possible to call a 900 number from a payphone using a red box somewhere in this country? It doesn't work in my area.

I enjoy your periodical a great deal (the phone articles are by far the best since access is universal). Keep up the good work!

Akron, Ohio

The COCOT (Customer Owned Coin Operated Telephone) you investigated is a very common one. Some others for our readers to *play with are at 602-820-1430, 516-467-9183, and 214-286-3334. It may take a good ten rings for them to answer with the computer voice and it might be hard to keep curious humans from picking up when you call. The four tones after the "Thank you" sound suspiciously like silver box tones (A, B, C, D) — we don't know what their purpose is. Obviously, the phone then waits for you to enter the right digits. Currently, we have no idea as to what the format is. Once we have that information, it'll be easier to crack and we can see just what these phones can do. We encourage our readers to evaluate the different types of payphones in their areas, get their numbers, call them, experiment, etc. Let us know what you find.*

Regarding 900 numbers from payphones: generally it doesn't work, not even 900-555-1212, which is a free call. But software errors in the central office can make wonderful things happen. There was a time when quite a few payphones in New York City would call ANY 900 number free of charge. You may find this in your area if nobody's caught it. You may find a COCOT that allows this. But don't expect it to last. Usually after the first bill rolls in, they figure out what's wrong pretty quickly. If you are lucky enough to find one of these holes, you'll soon discover how boring most of these services are, even for free. And then you won't have to worry about falling for that crap in the future. It's too bad the general populace can't share that realization.

GTE Mysteries

Dear 2600:

I'm the kind of guy that likes to just try things for the hell of it (what's this button for??). You know, to see what happens or just for the sake of knowing something new, even if it's "useless". Anyway, that's how I stumbled upon this little telephone episode.

I live in the "south bay" region of Los Angeles and my phone company is the infamous GTE. Just recently, I had the "Smart Pack" features (call forward, call waiting, call conferencing, and speed calling) added to my service. Anyway, I dialed my own number, for whatever reason, and much to my surprise, I did not get a busy signal. What I got instead were four short beeps (sounding just like "conversation being recorded" beeps) spaced apart about a half second each. Then I'm disconnected and just dead silence. I waited a few seconds, pushed assorted buttons, nothing. Then a nice steady tone like one would get calling a long distance 800 number. Not knowing why, how, or what to do, I just pushed more tones. Nothing. Then the nasty "line off the hook" tone comes blasting through, so I hung up.

Are you familiar with an incident such as this? Is this related to the Smart Package? GTE? Freak of nature? Sorry I can't tell you what ESS is in use here. If you haven't already guessed, I am a novice at phone hacking.

By the way, I love your publication, filled with neat stuff I may never use but still fun to read.

Some thank you info: 114 in my GTE area gets the computer voice readout of the number you're calling on, and I've been told 1223 does likewise for PAC-TEL.

H.
Manhattan Beach, CA

It sounds like you came in on your own call waiting. That could explain the four beeps. We don't know why you were disconnected, however. GTE has a lot of oddities and we'd love to hear about some more of them. For instance, WHAT "nice steady tone like one would get calling a long distance 800 number"? We in non-GTE land have never heard of such a thing, which you probably take for granted.

On Being Traced

Dear 2600:

There's a question that every hacker has asked at least once in his life and I am surprised that you have not as yet covered it. When hacking onto a system, everybody always wants to know "Who does the system belong to?" and "Does this system trace?" The answer to the first one should be obvious. CNA's have always proven to be very useful here. But what about the second question? How common is it for a mainframe to have tracing equipment on it, and after hacking it for some time, is it possible, if the company detects you, for them to obtain tracing equipment to catch you, and if so, how likely do you think it is that they will obtain such facilities? The reason I ask this is that I often scan exchanges looking for computers to hack and I often wonder how "safe" a system that I am playing with is.

The CPU Raider

We've covered this many times. Any system, be it a phone system or a computer system, can install a trace if abuse is suspected. It is not wise to call any system directly from your home for just that reason. Calling an extender to reroute your call to a computer system won't do you much good if the extender people put a trace on THEIR system! But don't let us mislead you. There are always ways to get in and STAY in if you're good, determined, and smart.

Information

Dear 2600:

Do you still have 2600 t-shirts?

KS
Pittsburgh, PA

Not at the moment. Hopefully by the time the Spring issue comes out, we'll have a new run.

Dear 2600:

I was wondering what the address was for the Chaos Computer Club in West Germany.

DS
Rocky Point, NY

Chaos Computer Club, Schwenckestr 85, D-2000 Hamburg 20, West Germany. Phone number from the States: 011-49-40-4903757.

Dear 2600:

To complete my collection of 2600 Magazine I have back issues for 84, 85, 86, 87, and parts of 88

send us your letters and comments

and 89 to date. What I need to know is:

Are there other back issues of 2600 beyond January 84?

In 88 I started with the Summer issue. What issues in 88 preceded these? Are they available? What is the cost?

Would anyone out there happen to know the current address to WORM Magazine, or if it still exists?

AG
San Bernardino, CA

1984 was our first year of publication and so there are no back issues before then. For 1988 and 1989, it is possible to buy single back issues for $6.25 each domestically, $7.50 overseas. We don't sell individual back issues before 1988 because we were a monthly publication and the space needed to keep a ready supply of EVERY individual issue is beyond our abilities. That's why we offer only the package deal for 1984 through 1987.

It appears that WORM Magazine doesn't exist, as mail to the address we published has been coming back combined with the fact that we haven't seen an issue for quite some time. The best way to find out is by reading Factsheet Five, a magazine that reviews other magazines (yes, we're in there) and gives you a good idea of the diversity that's available. You can write to them care of Mike Gunderloy at 6 Arizona Ave., Rensselaer, NY 12144-4502 or call 518-479-3707. A single copy costs $3 in North America, $7 elsewhere.

Life's Little Moments

Dear 2600:

Although I have only recently come in from the cold to what I feel to be old friends at 2600, I would want you to know I've had great respect for your work over the years. Our old network was Cloud Nine (it went down in November of 1978), the head master of which was Honest Abe of Kentucky.

Now that we have put "old blue" on the shelf, I want to ask the proletarial for their best shot at our new "system" here at the old sin din. It was hatched by our group of Sigma Pi Sigmas here on campus. The idea was born when MA bought our local wire chef a new reflectascope+spectrum analyzer. It is a real dream machine and we have all had plum playing "footsy" with him. Fortunate-ly/unfortunately he missed the part about capacitive reactance in his ICS courses. Our link is a cordless phone tapped in through a mercury wetted reverse current breakpoint to the payphone up the block. This is so when John Q. Public goes off hook to use the payphone it drops us off automatically (we work the BBS's at night anyway). So far we have lost only the bottom half of a Southwestern Bell Freedom Phone and the breakpoint relay (we hid it better this time). Around here MA has never been into Radio Direction Finding (until Cell Phones) so we have had it pretty easy. The only sad part is when we hear the screams of the sysops on the other end of the voice line. Is MA working on them with cattle prods these days? In the past our RF link was 2 meter HAM band but if you lose one of them it can be quite a bit more expensive than the loss of half a Freedom Phone 1700. We use most anything to punch our modems through the top half of the cordless phone (I use my old "TRASH"-80 4/P with a Teletrends Corp. TT512P 1200 baud — so I don't have that much to lose.) I use Omniterm with BIG RED (quarters only) on board.

The wire chef uses 2 Kc. to ping with his new reflectascope so we use a good tight notch pass bridge filter with H pad resonant coupling to let him go by. The tie point can we use at the pay phone happens to be a regular rats nest and this helps hide things. Also we use #32 wire for the physical tap (he wears trifocal glasses and hasn't seen anything that small in about five years now). We also have a drop weight fixed just out of sight so when he lifts up the can lid it rips out our tap lines and slipshuts the bypass filter and H pad resonant LC coupler (both together are about the size of a Tootsy Role) over the top of the pole into the next county.

I greatly enjoyed reading the back issues of 2600 and will order the rest of them when I get time and cash.

Your Bastard Stepchild
and Friend,
F.M. "Cordless"

We enjoyed reading your letter. It's not often we hear from your particular universe.

Fun Numbers

Dear 2600:

Here in New York City the whole 959 prefix is dedicated to test numbers and lots of other interesting stuff. The neat thing about this number is that it is free to call. Either at home or on a payphone the call costs you nothing.

Another interesting number can be found at 212-439-3200. That's the Lenox Hill Hospital health hotline. Using a touch tone phone, you can enter three digit codes and get medical information on over 300 topics. Each message is between three and five minutes and has been approved by Lenox Hill Hospital physicians. If you want a list of all of the topics, you can call 212-439-2980 to request a brochure.

The Seeker
New York City, NY

In addition to 959, the 890 exchange is full of test numbers for the phone company, all of which are toll-free. A good way to avoid the annoying repair service computer at 611 is currently 890-6611. A human answers now, but we're sure that that person's job won't last much longer. 890 is generally routed to the 315 area code in upstate New York, but if you call the one in your area code, you won't be charged. You might even see a call show up on your phone bill that says "TEST CALL" instead of the phone number. Don't worry, no charges will apply. Another oddity: up until recently, 890-TEST connected you to a strange service-order type of voice computer, and

we want to hear from you!

890-TONE hooked you into a modem of sorts. Both of those numbers are unreachable now, unless you dial them in area code 315, where they only work sometimes. We don't know what they're for, but you will be billed if you call them direct.

That hospital health hotline is a great service and it shows what slimebags the 900/dial-it service people really are. You don't need to charge a dollar a minute to provide a service. This hotline is yours for the price of a phone call. Let's hope for more of them.

Words of Thanks

Dear 2600:

Thank you very much for both 2600 and for the Central Office BBS — using info derived from them, I was able to gain vengeance against some sleazy Arizona computerniks who got me fired from my job. Perhaps you would not agree with my methods, but I feel justified (to say the least) in using extreme measures against a gang of out-and-out *criminal* hackers, in a city where all the cops are corrupt....

The ANI for the Sacramento area (916 area code) is 830-xxxx where xxxx is any four digits. (1111 works in most of the city.) Ringback is 970-xxxx.

If you print this, *please don't* use my name!!! I have *good reason* not to be connected with the above. Thank you very much.

???

As your letter came unsigned and without a return address, there really wouldn't be a way for us to print your name, would there?

How?

Dear 2600:

How is it possible to publish hacking and phreaking information without those in authority changing those systems you expose?

WAFB
Knob Noster, MO

Good question. Sometimes the systems are changed, sometimes some of them are changed, sometimes none of them are changed. But what we get out of it is the knowledge of how the systems operate and that's an invaluable tool which leads to our figuring out still more of them. In other words, knowledge and information are always advantageous and should never be stifled.

Hacker Clubs

Dear 2600:

In your Autumn 1989 edition you mentioned that you thought the hack/phreak spirit in the USA was dying. I agree, but would there be a way to start an open hack/phreak group similar to Chaos Computer Club? If you want you could call it 2600 and advertise in the Marketplace for people to start the clubs in their areas. They could have meetings similar to the ones you have once a month on Fridays.

EK
Syracuse, NY

We'd like for that to happen, but we can't wave our wands and expect it to occur just because we want it to. There has to be a desire from various people in various places. We can inspire that but we can't control it. It would be nice if people all over the world had meetings/get-togethers on the first Friday of the month. Ours have been going quite well and recently we've been having hackers from Europe call us on the payphones at Citicorp. We invite anyone to do this. Those payphone numbers are: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162, and 212-308-8184. We're there on the first Friday of every month between the hours of 5:00 PM and 8:00 PM, Eastern time. A warning: many strange people come to our meetings, so you may get an unpredictable response when you call. You may even get a regular person who knows nothing about 2600. We guarantee nothing.

Another Rip-Off Story

Dear 2600:

I thought the following might be interesting to you. I recently attended a State Fair. At one of the booths at the fair, there was a group of Sprint representatives asking people to sign up for a free FON card. All the person had to do was sign a slip of paper. However, by signing that slip of paper, the person also agreed to make Sprint their primary long distance carrier. The representatives really downplayed that fact; they highlighted with a pen all the phrases that contained "FON card", but the part which stated that Sprint would be made the long distance carrier was not highlighted, and in smaller print. I asked if I could have a FON card without making Sprint my primary long distance carrier, and they said that I would need a credit card for that. Well, I wasn't about to let these bums see it, so I declined on the deal. I wrote a letter to the BBB complaining about their tactics. My complaint was forwarded to Network 2000 Communications Corporation, an independent marketing company that is authorized to sell US Sprint services to residential and small business customers. Here is part of their reply:

"A large majority of customers that Network 2000 Independent Marketing Representatives obtain for US Sprint are acquired at fairs, flea markets, malls, etc. Network 2000 representatives are required to attend a thorough training program to learn proper, professional steps to obtaining customers for US Sprint before beginning their Network 2000 business. The method of obtaining customers used by a probable Network 2000 IMR which you described in your letter is *totally* against Network 2000 policy. Once we determine the name of the IMR, if we determine he acted unprofessionally, we will take swift action in terminating the individual's status as a Network 2000 IMR."

By the way, the ANI for Everett, Washington, which is served by GTE, is 411.

Dr. Williams
Washington State

If more people did what you did, this kind of rip-off would soon disappear. Unfortunately, you can

(continued on page 46)

(continued from page 19)

USING AND ABUSING WITH PRIMOS

```
  >editor. Heh. Ok, lets see what
Damn! No wordwrap. Remember, press
  >RETURN at the end of each 79
characters, ok? Now, lets go to EDIT
  >mode...

EDIT
wow
BAD WOW

INPUT
oops! "wow" is not an ED command! I'll
  >discuss ED's EDIT mode
commands in a few minutes. Let's quit!

EDIT
q
FILE MODIFIED OK TO QUIT? y
OK,
```

Okay, we are back at the PRIMOS command line. Damn! We forgot to save our newly-created text! What do we do now! Don't panic. Your text is still floating around in PRIMOS' memory. To restore your ED session, type:

OK, start 1000 (continues from break)

or

OK, start 1001 (resume in EDIT mode)

So, let's test it out, shall we?

```
OK, start 1001
EDIT
file sample_text
q
OK,
```

A few comments are now in order. Normally, when done with a document you would FILE the text away and then QUIT. If you try and QUIT without saving new text or changes made to text, you will be told that the file has been modified and asked for verification to quit. Should you make a "boo-boo" you can save your text by using one of the START command variations. The two EDIT mode commands we have just learned are:

FILE (abbreviated FIL) - files your text to the current UFD

QUIT (abbreviated Q) - exit ED to the PRIMOS command line

An alternate command to save your text is the SAVE command (abbreviated by SA). I prefer SAVE to FILE because SAVE is also used on my microcomputer. Use whichever you prefer, however.

A great feature of the START command will now be illustrated. Say you are moving around UFD's and you end up trying to create a file in a directory that you don't have W (Write) access in. Oh no! How do we save this new CPL program we just created? Simple! Using techniques that you have just learned, you can move to a different UFD (one that you have W access in) and save your text there. First, get into EDIT mode and QUIT the EDitor. From the PRIMOS command line, use the OR command to get to your "home" UFD or ATTACH to a different one and then issue the START 1001 command. Now FILE your text. Voila! A nice trick for the forgetful.

We now know the very basics of the PRIMOS line EDitor. We can create new files from scratch, append text to existing files, save or abort our modifications, and recover our text if we accidentally quit or hit the BREAK key (or send a BREAK signal). What we don't know is how to edit the text within an existing file or how to insert/delete text from an existing file (which is really easy). So read on!

PRIMOS normally uses the ? and " (double quote) as the kill and erase characters, respectively. So typing a ? in INPUT mode will kill the entire line. A " will similarly erase the previous character. I find the ? and " characters integral in my documents and you probably will too. The fix? Simple. From the PRIMOS command line (OK,), type:

```
term -erase <Ctrl-H>
term -kill _
```

Press CONTROL-H where it says "<Ctrl-H>". This will make the erase character a backspace and the kill character the DELETE key. Substitute whatever characters you feel most comfortable with on your microcomputer.

The semicolon character at the end of a line (;) will force a linefeed (as if you had pressed RETURN instead). You can end a line with either RETURN or a semicolon (useful if your RETURN key is broken?). If you enter a line of text containing semicolons such as this:

```
line one;;line three
```

ED will take it and output it as this:

```
line one
line three
```

Depending upon the location of the semicolon it may produce a linefeed or a mode switch. Thus, the line of text:

```
This is a caveat;
```

will switch you from INPUT mode into EDIT mode. Avoid having semicolons at the end of a line of text. I will detail the method you will have to use to get around this if you want to have semicolons in your file.

Should you wish to edit/ insert/ delete lines of text within an existing file you will have to learn how ED addresses text in its buffer. I'll assume that you have loaded a file into ED and are in EDIT mode. The basis of our example:

```
OK,ed example_file
EDIT
```

Now let's view the entire file:

```
p 9999
.NULL.
This is the text of the file we are using
  >in our example.
I will change this file around so that you
  >will see how
to edit/ add/ delete text in a file.
.NULL.
BOTTOM
```

This example used "P 9999" to display the contents. "P" is the abbreviation for the PRINT command. So you see, I told ED to PRINT the first 9999 lines of the file in it's buffer. PRINT displays the specified number of lines (9999 in the example) and makes the last line displayed the "current" line.

The .NULL. is not a part of the file, but rather a marker. It marks a place where you can insert text. BOTTOM indicates that you are at the bottom of the file. Should you type PRINT (or P) again it will simply say: .NULL.

You can type PRINT (or P) by itself without a numeric argument. PRINT has a default value of 1. Conversely, a PRINT -n ("n" being a whole number) command will cause ED to display the file backwards.

To get to the top or bottom of a file, type:

top (Abbreviation is T)

or

bottom (Abbreviation is B)

Very simple. To see what the line number of the current line you are pointing to is, type:

```
where
BOTTOM
```

Since we did that PRINT 9999 command we are at the BOTTOM of the file. Let's go to line 2. Type:

```
point 2
```

This will set the ED pointer to line number 2. ED will tell you that you are at line 2 by displaying line 2 on your screen. You can abbreviate the POINT command by typing PO instead. Now try the WHERE command (it also has an abbreviated form, which is W). Type:

```
w
LINE 2
```

We now know how to move around in a file and display some or all of the lines of text it contains.

The NEXT command (abbreviated by N) will move the pointer down the specified number of lines towards the BOTTOM of the file (assuming that the specified number is positive). Negative numbers will move the pointer up. As per the PO command, the new pointer line will be displayed. Here are two examples:

```
n 1
to edit/add/delete text in a file.
n -2
This is the text of the file we are using in
  >our example.
```

To find text in the buffer, use the LOCATE command (abbreviated L). For example, to find the string "change this file" type:

```
l change this file
I will change this file around so that you
  >will see how
```

Now look and see where you are. Type:

THINGS TO KNOW ON A PRIME

```
w
LINE 2
```

Aha! The LOCATE command not only finds the specified string, but sets the pointer to the new line. Now, try and LOCATE the string "Aunt Jemima". Type:

```
l Aunt Jemima
BOTTOM
```

ED could not find the string in the text. The new pointer is BOTTOM, meaning that you are at the last line in the file.

Similar to LOCATE is the FIND command (abbreviated F). FIND only checks to see if the specified string is at the beginning of a line (i.e., the first character is in column 1, the second in column 2, and so forth). Here is an example:

```
find to edit/add
to edit/add/delete text in a file.
```

> "Read people's word processing documents, see what's in their databases."

As with LOCATE, FIND displays the line and resets the pointer to its new location. If the string is not found, FIND returns with BOTTOM and sets the pointer to the bottom of the file.

NFIND is a similar command which works in the opposite manner of the FIND command. NFIND (abbreviated NF) will locate the first line below the current line which does not begin with the specified string. In the following example, I'll display use of the NFIND command as well as display the method you may use to have multiple ED commands on one line:

```
EDIT
p3
.NULL.
This is the text of the file we are using in
  >our example.
i will change this file around so that you
  >will see how
to edit/add/delete text in a file.
top, nfind This is
I will change this file around so that you
  >will see how
```

As you can see, NFIND only finds the first line that does not start with the specified string. Also note the use of the comma as a command delimiter when issuing the TOP and NFIND commands. Just like with LOCATE and FIND, NFIND will also return BOTTOM and set the pointer to the end of the file if it cannot find a line not starting with the string you specify.

You can also FIND and NFIND string patterns on a line starting at a column position other than 1. The format for this option is displayed below:

```
f(8) change this file
I will change this file around so that you
  >will see how
```

The parentheses are required and there cannot be any spaces between the command and the (#).

To append text to the end of the current line, use the APPEND command (abbreviated with A). To append " 02/24/89." to the end of the last line, type:

```
po3
to edit/add/delete text in a file.
a  02/24/89.
to edit/add/delete text in a file. 02/24/89.
```

You must have a space between the APPEND command and the string you wish to append. If you had instead typed:

```
a 02/24/89.
```

you would have gotten:

```
to edit/add/delete text in a file.02/24/89.
```

Use the CHANGE command (abbreviated C) to change a string in the current line. The first character after the CHANGE command is used as the delimiter. This is a more complicated command than most other ED commands. Format:

CHANGE/string-1/string-2/[G] [n]

"string-1" is the original string and "string-2" is the replacement string. G specifies a global change. If G is omitted then only the first occurance of string-1 will be changed. "n" is a pointer value. If it is 0 or 1 (default values) then the change will be made to the current line (assuming the G option is not in use). If "n" is a value other than 0 or 1 then ED will inspect and make changes on "n" lines starting at the current line. As usual, ED will reset the pointer to the last line inspected. Should the file contain fewer than "n" lines, ED will make the specified changes in all the lines of the file and end by saying BOTTOM.

Should you wish to change a string containing slashes (/), CHANGE's delimiter character, then substitute a new delimiter character. Examples:

```
f 02
to edit/add/delete text in a file. 02/24/89.
change:02/:01/:
to edit/add/delete text in a file. 01/24/89.
c#/#-#
to edit/add/delete text in a file. 01-24-89.
c/01-24/24-Feb/
to edit/add/delete text in a file. 24 Feb 89.
```

You should always issue the TOP command prior to making global like changes.

To insert characters at the beginning of a line, use CHANGE like this:

```
po3
to edit/add/delete text in a file. 24-Feb-89.
c//Last Line —> /
Last Line —> to edit/add/delete text in a
  >file. 24-Feb 89.
```

Remember our dilemma with the semicolon character (;)? Say you want to have semicolons in your file. First, let's mark where we want ED to put the semicolon. Do this:

```
po3
Last Line —> to edit/add/delete text in a
  >file. 24-Feb-89.
c/. 24/@ 24/
Last Line —> to edit/add/delete text in a
  >file@ 24-Feb 89.
top, c/@/;/g9999
Last Line —> to edit/add/delete text in a
  >file; 24-Feb-89.
```

If you know where you want your semicolons from the start then just use a character that you don't plan on using elsewhere in the file (like the @ character) and place them where you desire. Then perform the above procedure. Voila! Instant semicolons when you thought it couldn't be done.

To delete commands from a file, use the DELETE command (abbreviated with D). I believe I don't like the second line of our example file. Let's delete it. To do this, type:

```
po2
d
top
p9999
.NULL.
This is the text of the file we are using in
  >our example.
Last Line —> to edit/add/delete text in a
  >file; 24-Feb 89.
.NULL.
```

No more line 2. As with other ED commands, DELETE deletes from the current line. DELETE 1 will not delete the first line of the file, but rather the current line. DELETE 5 will delete the fifth line from the current line (with starting line being the current line)

The last ED command I will go over is the RETYPE command (abbreviated with R). RETYPE will delete the current line and replace it with the specified string. Notice that the text of our example is now nonsensical. The second line is a sentence fragment. Let's fix this grammatical error.

```
po2
Last Line —> to edit/add/delete text in a
```

PRIME HACKING

```
>file; 24-Feb-89.
r Now you will learn how to
  >edit/add/delete text in a file.
Now you will learn how to edit/add/delete
  >text in a file.
```

RETYPE followed by a space and a RETURN will delete the current line. This will make a "null" line. This can be used as an alternate method for creating "null" lines (to delimit paragraphs in your text) as opposed to making the line a blank space.

Let's look at both the original example file and its present form:

```
ORIGINAL:
This is the text of the file we are using in
  >our example.
I will change this file around so that you
  >will see how
to edit/add/delete text in a file.
CURRENT:
This is the text of the file we are using in
  >our example.
Now you will learn how to edit/add/delete
  >text in a file.
```

The most useful means of using ED is to upload text (documents or sources) to the host Prime. Simply load in the file on your microcomputer and go into your terminal program's editor. Change all occurances of a null line to a space and a RETURN. Now enter ED and upload your file via the ASCII protocol. You might need to lower the sending speed (the line delay) if you seem to be sending text too fast for ED to get it. When done with the send, just enter EDIT mode and SAVE or FILE the text.

WARNING: If the filename you specify ED to save your text as exists in the current UFD then ED will overwrite the file with the text in its buffer. Be careful not to use an existing filename when you save files or you might be sorry.

Now for some important notes on PRIMOS filenames.

1. Filename can be up to 32 characters long.

2. Filenames can only contain the following characters: A-Z, 0-9, & - $. _ / #

3. The first character cannot be a number.

4. No embedded blanks or special characters (like [ ] { } [ ] etc).

5. All characters are mapped to UPPER CASE by PRIMOS.

Legal Filenames

```
MYFILE
TODAYS-SYSTEMS
$MONEY
TEXT_FILE
PRIMES&VAXEN
```

Illegal Filenames

```
MY FILE
SYSTEMS?
4MONEY
ACCTS@PRIME
"COOL"
```

NOTE: ED does not like TABs! Do not use your terminal's TAB key! ED will not understand them. To tell ED to use a TAB, use the backslash (\) character. Example:

tab\this\out\for me.

will insert tabs where the \'s are.

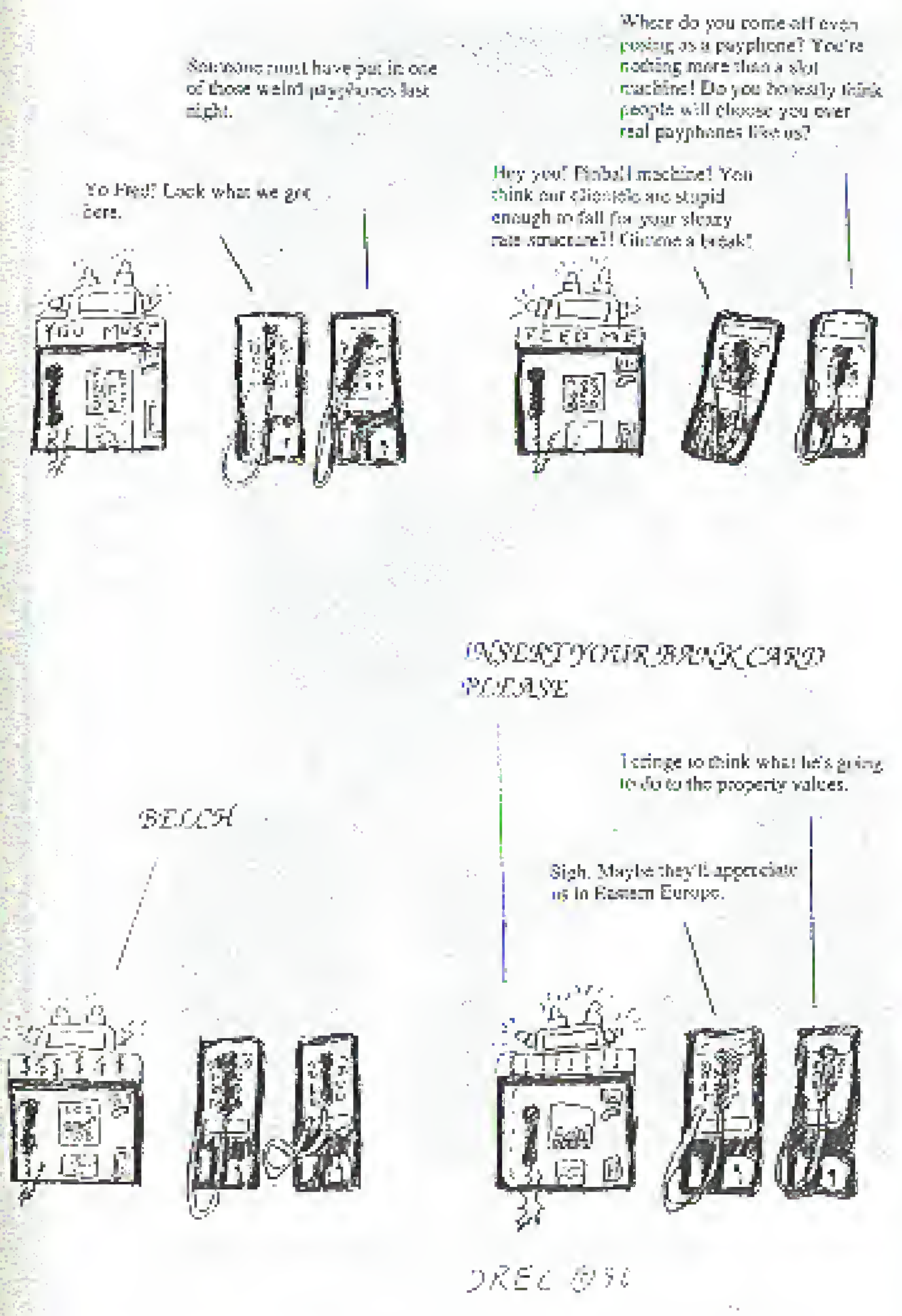
EDitor has many other commands. Type HELP ED to obtain a list of them and a brief statement of each one's function.

Experimentation With Other PRIMOS Applications and Utilities

There are many other applications that you will find on Primes. Some of them useful and interesting, some of no use whatsoever to the hacker. I can't begin to describe them here. This part of the series is already larger than I had planned, so I am going to have to end it here. Here is a very incomplete list of applications commonly found on Prime computer systems:

PRIME INFORMATION - A database system
PRIME WORD - A word-processing system
MIDAS - A graphics design utility
TELL-A-GRAF - A graphing utility
ORACLE - A database system

There are tons more applications systems to be found on Primes. Experiment! It is best to experiment with available applications to see if they can be useful. Read people's word processing documents, see what's in their databases. You never know what you might find! Just be careful not to delete or change anything!


Yo Fred! Look what we got here.
Someone must have put in one of those weird payphones last night.
YOU MUST
Hey you! Pinball machine! You think our clientele are stupid enough to fall for your sleazy rate structure!! Gimme a break!
Where do you come off even posing as a payphone? You're nothing more than a slot machine! Do you honestly think people will choose you over real payphones like us?
FEED ME
BELCH
INSERT YOUR BANK CARD PLEASE
I cringe to think what he's going to do to the property values.
Sigh. Maybe they'll appreciate us in Eastern Europe.
DREL '89

What arm's deal?

KEEP THOSE FAXES COMING!
516-751-2608

2600 Marketplace

WANTED: Red box kits, plans, and assembled units. Also, other unique products. For educational purposes only. Please send information and prices to: TJ, 21 Rosemont Avenue, Johnston, RI 02919.

RARE TEL BACK ISSUE SET (like TAP but strictly telephones). Complete 7 issue 114 page set. $15 ppd. Have photo copy machine self serve key counter. Would like to trade for red box minus its IC'S. Pete Haas, P.O. Box 702, Kent, Ohio 44240.

THE CHESHIRE CATALYST, former editor of the TAP newsletter, has dates available to lecture in Europe in late August and early September. For lecture fees and information on seminars to be given, write to: Richard Cheshire, P.O. Box 641, Cape Canaveral, FL, USA 32920.

TENTATIVE DATES for Summercon 90: June 22-24. Watch this space.

CYBERPUNKS, HACKERS, PHREAKS, Libertarians, Discordians, Soldiers of Terrane, and Generally Naughty People: Protect your data! Send me a buck and I'll send you an IBM PC floppy with some nifty shareware encryption routines and a copy of my paper "Crossbows to Cryptography: Techno-Thwarting the State," Chuck, The LiberTech Project, 8726 S. Sepulveda Blvd., Suite B-253, Los Angeles, CA 90045.

NEEDED: Info on speech encryption (Digicom Crypto). Send to Hack Tic, P.O. Box 22953, 1100 DL, Amsterdam, The Netherlands.

TAP BACK ISSUES, complete set Vol 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/45 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

HACKING AND PHREAKING SOFTWARE for the IBM and Hayes compatible modems. The best war dialers, extender scanners, and hacking programs. $8.00, including shipping and handling. Make payable to Tim S., P.O. Box 2511, Bellingham, WA 98227-2511.

FOR SALE: Manual for stepping switches (c) 1964. This is a true collector's item, with detailed explanations, diagrams, theory, and practical hints. $15 or trade for Applecat Tone Recognition program. **FOR SALE:** Genuine Bell phone handset. Orange w/tone, pulse, mute, listen talk, status lights. Fully functional. Box clip and belt clip included. $90 OBO. Please post to S. Foxx, POB 31451, River Station, Rochester, NY 14627.

FOR SALE: DEC VAX/VMS manuals for VMS 4.2. All manuals are in mint condition, some still in the shrink-wrap. This is the best source for VMS knowledge anywhere! Contact me for more info. Kurt P., POB 11282, Blacksburg, VA, 24062-1282.

WANTED: Schematic and/or block diagram for G.E. TDM-114B-13 data set. John B. Riley, 914 N. Cordova St., Burbank, CA 91505-2925.

UNDERGROUND BOOKS: TAP, complete set, volumes 1-91, $80. Electronic surveillance and wiretapping -- a nuts and bolts guide, $15. The best of TAP, over 100 pages of their best, $40. Computer crime, over 400 pages from the best of government publications, prosecutors' guides, documents, case studies, etc., including how it's done, $60. Include $3 handling per book. Make payment to Tim S., PO Box 2511, Bellingham, Washington 98227-2511.

2600 MEETINGS. First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E. 53rd St., NY, between Lex & 3rd. Come by, drop off articles, ask questions. Call 516-751-2600 for more info. Payphone numbers at Citicorp: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8152, 212-308-8184.

Deadline for Spring Marketplace: 3/1/90.

Do you have something to sell? Are you looking for something to buy? Or trade? This is the place! The 2600 Marketplace is free to subscribers! Send your ad to: 2600 Marketplace, P.O. Box 99, Middle Island, NY 11953. Include your address label. Only people please, no businesses.

what's happening

(continued from page 8)

the tone. Under the new system: thirty seconds after the tone. You know where this company's priorities are, don't you?

Ripoff City

Add Cable and Wireless (TDX) to the list of long distance companies ripping off their customers with AOS operators. If you dial a zero plus call on a line that's selected Cable and Wireless as its long distance company, you'll hear an AT&T-like tone, but you'll wind up being connected to NTS. To give you an example of where NTS is coming from, they refused to give us their rates until we gave them our card number. When we have managed to get rates from them, they were often more than double those of AT&T's. MCI did the same thing about a year ago, then suddenly stopped after the media got wind of it. And ITT has been using the ITI company to process its operator assisted calls. Not only are they ripping people off, but they're confusing them with the similar sounding names! Cable and Wireless won't process any calls on its 10223 code unless you've signed up with them. ITT processes calls on both 10488 and 10999 regardless of whether or not you've signed up with them. To get ripped off, just dial a zero plus the number you're calling after entering one of the above codes.

***

New York State officials are warning lottery players that a telephone hotline for winning numbers is charging more than three times the cost of a lottery ticket for each call. According to a representative of the State Lottery, Buffalo Audiotex Inc. bills callers $3.50 to find out nothing more than the previous night's winning numbers, information readily available for free. The company also doesn't bother mentioning the price during the course of the call. But the best part of it is that, according to the New York Public Service Commission, it's all completely legal.

Calling London

London is bracing for a major catastrophe: a city code change. On May 6th, the city code of 01 will be split in half. Inner London will change to 071 and the rest of the present 01 area will change to 081. For people calling in from outside the country, the leading zero is always dropped, so the code will be changing from 1 to either 71 or 81. Not much of a hassle from over here in the States, but inside London it's another story. If you need to call from one part of London to another, instead of dialing seven digits, you will soon have to dial ten. Is nothing sacred?

Sprint Is Watching

Businesses using US Sprint can now get a free service to help them track down people who use their PBX's without authorization. Since Sprint is able to determine where calls to their network are coming from, they're more than willing to disclose this information. US Sprint uses Northern Telecom DMS-250 switches coupled with Feature Group D access capability in central offices to identify the originating numbers of all network calls. Welcome to the nineties.

Equal Access For All

Prisoners at the State Correctional Institute in Dallas, PA managed to install and use telephone service at a remote location. They obtained credit information on a number of prison correctional officers. Using this information, they had lines installed in those names at a house in Philadelphia. When an inmate called one of the numbers collect, an acquaintance at the house would three-way them into the number they wanted to call. The total bill came to around $12,000.

German Democratic Phones

According to industry experts, most of East Germany's severely strained phone network is beyond repair and needs a complete overhaul. The network has been in place since before World War II. However, during the events of November 9, the network virtually collapsed. Several West German companies have expressed an interest in rebuilding the system. West Germany has about 40 million telephone lines and a population of about 60 million. East Germany, with 17 million people, only has 4 million phone lines. The quality of service is also poor, and "self-dialing" is virtually unknown outside of East Berlin.

Too Much Chatter

Prodigy, the IBM-Sears joint venture for personal computer users, has gotten rid of something it apparently doesn't want: controversy. The $10 a month service gives users access to shopping services, stock market reports, and airline reservations. But it also has bulletin boards that let subscribers communicate with each other. One of these boards, known as Health Spa, turned into a debating ground between homosexuals and fundamentalists. That was too much for Prodigy, who discontinued the service in December because, according to them, it wasn't generating enough interest. This despite the fact that the board generated far more traffic than many of the other "successful" boards.

the npa countdown

From a recent Bellcore V&H Tape, here is a list of all North American area codes and the number of exchanges being used in each. Delaware (302) has the fewest with only 57 in use. Both 212 and 213 area codes are nearly full enough to split for the second time. In a couple of years, area codes will no longer have to have a 1 or a 0 as the middle digit. Depending upon how this is implemented, the effects could be quite traumatic.

Format is area code: number of exchanges within.

201: 562
202: 556
203: 445
204: 384
205: 583
206: 510
207: 375
208: 263
209: 297
212: 624
213: 667
214: 671
215: 555
216: 521
217: 541
218: 258
219: 529
301: 553
302: 57
303: 464
304: 315
305: 427
306: 426
307: 137
308: 189
309: 250
312: 729
313: 596
314: 436
315: 266
316: 245
317: 358
318: 331
319: 332
401: 126
402: 392
403: 375
404: 613
405: 475
406: 325
407: 335
408: 266
409: 263
412: 459
413: 126
414: 422
415: 582
416: 572
417: 249
418: 246
419: 319
501: 517
502: 329
503: 481
504: 305
505: 283
506: 157
507: 251
508: 339
509: 324
512: 576
513: 448
514: 445
515: 385
516: 439
517: 333
518: 336
519: 326
601: 378
602: 552
603: 213
604: 372
605: 322
606: 250
607: 158
608: 226
609: 250
612: 492
613: 262
614: 370
615: 434
616: 349
617: 336
618: 311
619: 435
701: 141
702: 247
703: 519
704: 310
705: 351
706: 159
707: 160
708: 425
709: 245
712: 264
713: 474
714: 504
715: 294
716: 347
717: 459
718: 325
719: 185
801: 303
802: 171
803: 467
804: 446
805: 252
806: 236
807: 103
808: 225
809: 449
812: 255
813: 448
814: 250
815: 275
816: 428
817: 443
818: 312
819: 295
901: 226
902: 245
904: 366
906: 106
907: 337
912: 306
913: 417
914: 311
915: 375
916: 371
918: 274
919: 633

Now here's the same list showing the least-populated area codes followed by the most-populated. The area codes at the bottom of the list are the ones most likely to split off in the near future. A few are already in the process of doing this.

Format is number of exchanges: area code.

57: 302
103: 807
106: 906
120: 431
126: 419
137: 307
146: 718
157: 506
158: 407
159: 706
161: 707
171: 802
182: 308
189: 417
205: 901
219: 603
224: 509
226: 608
226: 609
226: 519
236: 806
240: 719
245: 902
249: 902
247: 702
252: 305
253: 605
255: 805
256: 814
251: 527
253: 726
256: 606
259: 612
260: 905
262: 613
263: 208
263: 408
264: 712
265: 408
268: 218
271: 815
274: 918
275: 915
286: 503
294: 715
295: 819
297: 209
300: 601
303: 507
304: 504
309: 912
310: 704
311: 618
311: 914
312: 316
315: 304
319: 319
319: 419
320: 605
321: 318
323: 406
325: 201
326: 513
328: 502
329: 215
330: 617
333: 401
334: 204
337: 907
338: 608
338: 516
343: 217
343: 701
345: 216
347: 714
348: 418
349: 616
350: 719
351: 904
358: 317
359: 402
370: 604
380: 505
382: 402
400: 412
415: 708
417: 513
420: 414
422: 305
426: 306
428: 816
435: 619
445: 317
445: 203
445: 504
446: 805
449: 514
449: 802
449: 813
459: 717
464: 303
467: 803
468: 202
474: 713
475: 405
486: 503
488: 612
494: 214
596: 617
604: 714
610: 806
612: 531
615: 735
621: 215
623: 654
652: 602
655: 213
666: 212
670: 416
675: 451
676: 512
682: 415
683: 205
686: 313
602: 519
611: 404
624: 512
650: 201
620: 201
662: 213
671: 214
729: 312

This info comes from the Telecom Digest.

UAPC UPDATE

by The Plague

I certainly hope you enjoyed my article in the last issue. However the folks at UAPC did not. Needless to say, there was a big media scandal here in New York when 2600 hit the stands last fall. Certain individuals took it upon themselves to crack UAPC at any cost. As I predicted, social engineering and trashing were key elements used in cracking the system. At least one group of hackers was able to get access to more than a dozen accounts. They contacted people at 2600 who alerted the media. And for the first time in America, hackers were the ones to break a story about hacking. For once, the hackers had the upper hand, which greatly reduced the amount of inaccuracies in the story. It also made those in charge of the system look like utter fools.

The almighty school system got very angry and decided to take security measures. They claimed that they were going to put UAPC on leased lines by January 1990. Well, that hasn't happened, and even if it does happen, the next few paragraphs will show you how to get around that.

I myself enjoyed rubbing it in to UAPC, by placing certain foul stickers on their door as well as having some fun engineering their Help Desk while they were in a state of security alertness. "Hello, is this the UAPC Help Desk? Yeah? Well you certainly do need help!!" and things of that sort.

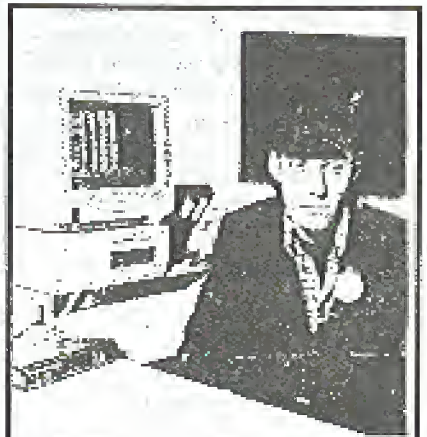
One thing that UAPC did which was very nasty was to place a Project ID on every single account. Now, that's not a big problem. If you can get the password, you can get the Project ID in the same way. However, one day I stumbled onto something interesting. I found out that you can connect to UAPC through the CUNY/UCC (City University of New York - University Computer Center). What's even better is that you can connect at up to 2400 baud and use the terminal emulation of your choice. But, the very best thing about it is that you don't have to provide a Project ID to UAPC if you connect via UCC. Apparently, the Project ID's are only used when UAPC is accessed via UAPC's own dial-up lines.

UCC is a computing server located in Manhattan. It provides high-speed network links (SNA) to many computers throughout the CUNY system. UAPC is linked via this high-speed network, and there is much less security when accessing UAPC via UCC.

Here is what you can do. UCC is a public number, so I might as well give it out. It's 212-974-8600 and connects at 300, 1200, and 2400 baud using 7E1 (seven data bits, even parity, one stop bit). Once connected, you hit RETURN a few times. It should ask for terminal type. You can hit return to see the available terminal types, and then choose one that your software can emulate. You will then see the UCC opening screen. At that point you hit the TAB key until the cursor is at the COMMAND line, then type DIAL VTAM and hit return. You will then see a menu screen of the computers that you can connect to. You keep hitting TAB (also known as Ctrl-I) until your cursor is at UAPC and then you hit return. You are now connected to UAPC. You will notice that UAPC only asks for User ID and Password. It does not ask for Project ID. The password input area is divided into three areas. The first is required. The other two are optional. The first input area is for the password, the second is for the password you want to change it to (if the password is valid), the third is to verify the change. You don't have to worry about that at all. You can just type the user name followed by return and then the password followed by return. As a side note on UCC, you can emulate the PF keys on your terminal by using the ESC key. For instance, PF1 is the same thing as hitting ESC and then 1.

So now you can see that even if UAPC does go on leased lines, which I'm willing to bet it will not, you can still access it via UCC. The reason that I think leased lines are out of the question is because it will severely hinder access for legitimate users all throughout the Board of Ed and CUNY.

Apparently, UAPC hacking and abuse has become a rather popular hobby here in New York. I'm constantly hearing rumors about people willing to pay cash for grade changes and people who can fill that particular service need.



A 2600 staffer demonstrates the ease of changing high school grades in a report aired over WNBC-TV in New York.

letters

(continued from page 33)

find these con-artists almost everywhere you look today. While Network 2000's response seems to indicate that they're concerned, the fact remains that they're blaming one person for this violation. But you said it was a group of representatives which would seem to indicate that what they were doing was company policy. It's also hard to believe that one person is responsible for reducing the size of the print on a key part of the advertisement.

Anyone involved in similar escapades? Let's hear about them.

And to add to the list of ANI (ANAC for those who want to be technical) numbers, try 1-200 followed by almost any seven numbers in the 305 and 407 area codes in Florida. Also, dialing 511 from many phones there will disable the phone for at least two minutes.

We know you have something to say to us! So write us a letter now before it slips your mind. Our address is 2600 Letters, PO Box 99, Middle Island, NY 11953. Our FAX number is 516-751-2608. Our new network address is 2600@well.sf.ca.us.

at&t

(continued from page 5)

network if something strange and unpredictable starts occurring. The news here isn't so much the failure of a computer program, but the failure of AT&T's entire structure.

The Non-Technical Problems

In the height of the crisis, Laura Abbott, an AT&T spokesperson, said callers shouldn't try using any of the other companies. She recommended repeated tries over AT&T. "If you don't get through the first time, you'll get through the second time."

AT&T operators, hours after the crisis began, refused to tell customers how they could place their calls over other long distance companies. It went against company policy. This, despite the fact that most long distance companies tell the customer how to access AT&T if he/she needs to.

The media once again let us down by not doing enough to educate themselves, let alone the public. All that had to be done was to alert the public as to how to make a long distance call using another company. Nobody had to be inconvenienced on that day.

Breaking up the Bell system was essential in the name of fairness. But it doesn't end there. The general public has to be educated on how to use the new system to their advantage. What good is a fair system if most people don't know how to use it? Why are people so afraid to do this? Why are they discouraged?

Many institutions and businesses choose to block access to the 10XXX system, thinking that somehow it will generate more bills. Many of them now realize belatedly the usefulness of that system.

The carrier access code list we printed in our last issue should be available to everybody in the country. Possession of this list is really the only way consumers will find alternative long distance companies that could be a life-saver in a situation like this.

During the California earthquake last October, AT&T made a decision for us. They decided that incoming calls weren't as important as outgoing calls to the people there. They were probably right. But, by blocking virtually all attempts, they were making a categorical assumption that simply doesn't hold up to individual reasoning. For those of us who knew the alternative ways to route our calls, calling in was no problem. But so few of us knew this.

There obviously have to be more alternatives, so that there are more choices for each of us. But there has to be a level of awareness among the end users, or else, what's the point?

NOW HEAR THAT

At 2600, we don't exactly go out of our way to nag you about when your subscription is going to stop. You won't find yourself getting those glossy reminders with free pens and digital quartz clocks and all that junk. We believe our subscribers are intelligent enough to look at their address label and see if their subscription is about to conclude. If it is or if you want to extend it, just fill out the form below (your label should be on the other side) and send it to our address (also on the other page). You don't get self addressed stamped envelopes from 2600. But the time and money we save will go towards making 2600 as good and informative as it can get.

INDIVIDUAL SUBSCRIPTION

☐ 1 year/$18 ☐ 2 years/$33 ☐ 3 years/$48

CORPORATE SUBSCRIPTION

☐ 1 year/$45 ☐ 2 years/$85 ☐ 3 years/$125

OVERSEAS SUBSCRIPTION

☐ 1 year, individual/$30 ☐ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

☐ $260 (you'll never have to deal with this anymore)

BACK ISSUES (never out of style)

☐ 1984/$25 ☐ 1985/$25 ☐ 1986/$25 ☐ 1987/$25

☐ 1988/$25

TOTAL AMOUNT ENCLOSED: ☐